
**DRDC No. CR2007-068**

# Interoperable Risk Management in a Joint Interagency Multinational Environment

by:

Barbara D. Adams, Sonya Waldherr and Kenneth Lee

Human*systems*® Incorporated
111 Farquhar St., 2nd floor
Guelph, ON N1H 3N4

Project Manager:
Dr. Barbara D. Adams
(519) 836-5911 ext 249

PWGSC Contract No. W7711-047911/001/TOR
Callup No. 7911-08

On behalf of
DEPARTMENT OF NATIONAL DEFENCE
as represented by
Defence Research and Development Canada Toronto
Toronto, Ontario, Canada
M3M 3B9

DRDC Toronto Scientific Authority
Dr. David R. Mandel
(416) 635-2000 ext 3146

August 2007


Author

Barbara D. Adams
Human*systems*® Incorporated

Approved by

Dr. David R. Mandel
[Enter title here]

Approved for release by

[Enter name here]
[Enter title here]

# Abstract

This report addresses risk management in the Department of National Defence and Canadian Forces (DND/CF), and explores the extent to which the DND/CF is likely to be interoperable internally (e.g., in joint operations), as well as in relation to other organizations in the event of a major threat such as a terrorist attack.

This report first explores existing national standards for conducting risk management, as well as the Treasury Board of Canada Secretariat's (2001) Integrated Risk Management Framework (IRMF) that mandates all government departments in Canada have a risk management plan. The available risk management approach of the DND/CF (available in existing doctrine) is then considered in relation to the approach mandated by the Treasury Board of Canada Secretariat. A review by the Chief Review Services (CRS) and Deloitte & Touche (2004) also provided a detailed assessment of the progress that the DND/CF had made in implementing an integrated risk management plan.

Review of these documents suggests some potential challenges to future interoperability in risk management approaches. Specifically, one potential problem (also noted in the CRS & Deloitte & Touche review) are the two distinct cultures within the DND/CF with respect to risk management, and these cultural differences were no less prominent in 2005 documents provided by the DND/CF in response to the CRS and Deloitte & Touche review. In general, the need for a common definition of risk management was also evident, as was a potential disconnect between the explicit risk management policies and the implicit approaches likely to be taken in an actual risk or threat situation.

Other articles were reviewed to explore the potential interoperability of the DND/CF in relation to other government departments such as Public Security and Emergency Preparedness Canada (PSEPC) and Health Canada. Reports published by the Office of the Auditor General of Canada, for example, showed that the progress of other government departments (OGDs) in working toward integrated risk management was slower than optimal (Office of the Auditor General of Canada, 2003). Even the specific departments charged with emergency preparedness had not established a clear chain of command, showed a lack of common standards and practices, and had not succeeded in achieving interoperability even in their everyday workings (Office of the Auditor General of Canada, 2005). These problems are likely to deter significantly from risk management efforts.

The final chapter of this report describes a research approach that would explore risk management within the DND/CF as well as in relation to other government departments likely to be implicated in responding to terrorist threats. Lastly, this report details the creation of research questionnaires that could be used to further explore these issues, and the questions that could be used in face-to-face interviews. Other possible research approaches are also discussed, including the development of risk management scenarios. Hopefully, the work undertaken in this report will provide a sound basis for future research working to understand and promote higher levels of interoperability in managing risk.

# Résumé

Ce rapport porte sur la gestion des risques au sein du ministère de la Défense nationale et des Forces canadiennes, et il montre dans quelle mesure le MDN/les FC sont susceptibles d'être interopérables à l'interne (p. ex., au cours d'opérations interarmées) et lorsqu'ils sont en relation avec d'autres organisations gouvernementales en cas de menace sérieuse telle qu'un attentat terroriste.

Ce rapport traite d'abord des normes nationales existantes en matière de gestion des risques, de même que du Cadre de gestion intégrée des risques du Conseil du Trésor (2001), qui oblige tous les organismes gouvernementaux canadiens à avoir un plan de gestion des risques. L'approche de gestion des risques actuelle du MDN/des FC (qui se trouve dans la doctrine actuelle) est ensuite examinée par rapport à l'approche rendue obligatoire par le Conseil du Trésor. Un examen effectué par le Chef – Service d'examen (2004) a également fourni une évaluation approfondie des progrès faits par le MND/les FC en ce qui a trait à la mise en œuvre d'un plan de gestion intégrée des risques.

L'examen de ces documents suscite certaines préoccupations en ce qui concerne l'interopérabilité future. Plus particulièrement, les deux cultures distinctes présentes au sein du MDN/des FC en matière de gestion des risques constituent un problème potentiel (également indiqué dans l'examen du CS Ex), et ces différences culturelles n'étaient pas moins évidentes dans les documents qu'ont fournis le MDN/les FC en 2005 en réaction à l'examen du CS Ex. En général, le besoin d'une définition commune de la gestion des risques était également évident, comme l'était la possibilité d'une rupture entre les politiques de gestion des risques explicites et les approches implicites susceptibles d'être utilisées dans une situation réelle comportant un risque ou une menace.

D'autres articles ont été examinés en vue d'étudier l'interopérabilité potentielle du MDN/des FC lorsqu'ils sont en relation avec d'autres ministères comme Sécurité publique et Protection civile Canada (SPPCC) et Santé Canada. Par exemple, des rapports du vérificateur général ont montré que les progrès accomplis par d'autres ministères quant au travail relatif à la gestion intégrée des risques étaient plutôt lents (2003) et que même les ministères particuliers chargés de la protection civile n'avaient pas établi une chaîne de commandement claire, n'avaient pas de normes et de pratiques communes et qu'ils n'étaient même pas interopérables dans leur fonctionnement de tous les jours (2005). Ces problèmes sont susceptibles d'avoir un effet dissuasif important relativement aux efforts en matière de gestion des risques.

Le dernier chapitre de ce rapport décrit une approche de recherche qui étudierait la gestion des risques au sein du MDN/des FC de même que lorsqu'ils sont en relation avec d'autres organismes gouvernementaux susceptibles de prendre part à la réaction à des menaces terroristes. Finalement, ce rapport décrit l'élaboration de questionnaires de recherche qui pourraient être utilisés pour examiner plus en détail ces problèmes, et il présente les questions qui pourraient être utilisées au cours d'entrevues directes. D'autres approches de recherche possibles sont aussi examinées, notamment l'élaboration de scénarios de gestion des risques. Il y a lieu d'espérer que le travail entrepris dans le cadre de ce projet fournira un fondement solide pour les travaux de recherche futurs visant la compréhension et la promotion de niveaux d'interopérabilité plus élevés en ce qui a trait à la gestion des risques.

# Executive Summary

This report addresses risk management in the Department of National Defence and Canadian Forces (DND/CF), and explores the extent to which the DND/CF is likely to be interoperable within itself (e.g., in joint operations), as well as in relation to other organizations in the event of a major threat such as a terrorist attack.

This report first explores existing national standards for conducting risk management. This includes standards created by the Canadian Standards Association (CSA), as well as those used in other countries. At the federal level, however, the Treasury Board of Canada Secretariat mandated in 2001 that all government departments must have an articulated risk management plan that seeks to integrate risk management into the daily workings of the organization. According to this document, integrated risk management refers to the "continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective" (p. 7). This approach to risk management is explored in some detail.

The available risk management approach of the DND/CF is then considered in relation to these standards, and to the approach mandated by the Treasury Board of Canada Secretariat. At this point, only the DND/CF doctrine related to risk management in the context of operational planning was available, but this provided a rich source of information about how the DND/CF understand risk management. In addition, a review by the Chief Review Services (CRS) & Deloitte & Touche, (2004) also provided a detailed assessment of the progress that the DND/CF had made in implementing an integrated risk management plan. In general, this review concluded that although some progress had been made (with some areas showing more progress than others), risk management within the DND/CF was still at a relatively early stage of development at the time of the publication of these documents.

Documents released by the DND/CF in 2005 (DND, 2005a; 2005b) seemed to form a response to some of the criticisms contained in the CRS and Deloitte & Touche (2004) review. Careful review of these more recent DND documents suggests that ensuring high levels of future interoperability within diverse elements of the DND/CF may be challenging. Key observations arising from this document review suggest that there are at least 2 distinct cultures within the DND/CF with respect to risk management. Specifically, operational risk and National Defence Headquarters/operation support cultures may be difficult to harmonize. This review also supported the concerns raised by the CRS and Deloitte & Touche about the need for a common definition of risk management that extends to actual use. In addition, there is a potential disconnect between the explicit approaches to risk management and the implicit approaches likely to be taken in an actual risk or threat situation. Moreover, even the more recent documents (DND, 2005a; 2005b) still emphasize a distinctly operational perspective on risk management that may be difficult to harmonize with other cultures within the DND/CF, or with other external organizations. Of course, these observations are only preliminary, but do indicate a need for further research to explore these issues.

Other articles were reviewed to explore the potential interoperability of the DND/CF in relation to other government departments such as Public Security and Emergency Preparedness Canada (PSEPC) and Health Canada. Reports published by the Office of the Auditor General of Canada (2003; 2005), for example, showed that the progress of other government departments in working toward integrated risk management was slower than optimal. Even the specific departments charged with emergency preparedness had not established a clear chain of command, showed a

lack of common standards and practices, and had not succeeded in achieving interoperability even in their everyday workings. These observations, then, suggest that although many government departments have made considerable efforts to adopt integrated risk management, fully realizing this goal will take more time and effort.

Certainly, considerable work remains to be done in helping the DND/CF to incorporate integrated risk management into their organizations. However, it is also critical that the Government of Canada (and, for the purposes of this review, the DND/CF) is not complacent in believing that interoperability is guaranteed even if each government department has an excellent standalone risk management approach.

The final chapter of this report describes a research approach that would explore risk management within the DND/CF as well as in relation to other government departments likely to be implicated in responding to terrorist threats, with the goal of advancing interoperability. Lastly, this report details the creation of research questionnaires that could be used to further explore these issues, and the questions that could be used in face-to-face interviews. Other possible research approaches are also discussed, including the development of risk management scenarios. This future research, hopefully, will help to identify areas in which risk management can be made more interoperable.

# Sommaire

Ce rapport porte sur la gestion des risques au sein du ministère de la Défense nationale et des Forces canadiennes, et montre dans quelle mesure le MDN/les FC sont susceptibles d'être interopérables à l'interne (p. ex., au cours d'opérations interarmées) et lorsqu'ils sont en relation avec d'autres organisations en cas de menace sérieuse telle qu'un attentat terroriste.

Ce rapport traite d'abord des normes nationales existantes en matière de gestion des risques, y compris les normes élaborées par l'Association canadienne de normalisation de même que les normes utilisées dans d'autres pays. Toutefois, en 2001, à l'échelle du gouvernement du Canada, le Secrétariat du Conseil du Trésor a rendu obligatoire pour tous les organismes gouvernementaux d'avoir un plan de gestion des risques articulé visant à intégrer la gestion des risques dans les activités de tous les jours d'une organisation. Selon le document en question, la gestion intégrée des risques (GIR) se définit comme « un processus continu, proactif et systématique visant à comprendre, à gérer et à faire connaître les risques du point de vue de l'ensemble d'une organisation ». Cette approche de gestion des risques est étudiée en détail.

L'approche de gestion des risques actuelle du MDN/des FC a ensuite été examinée par rapport à ces normes et à l'approche rendue obligatoire par le Conseil du Trésor. À ce moment là, seule la doctrine du MDN/des FC qui concerne la gestion des risques dans un contexte de planification opérationnelle était disponible, mais elle a constitué une source d'information importante relativement à la compréhension du MDN/des FC en matière de gestion des risques. De plus, un examen effectué par le Chef – Service d'examen (2004) a également fourni une évaluation approfondie des progrès accomplis par le MND/les FC en ce qui a trait à la mise en œuvre d'un plan de gestion intégrée des risques. De manière générale, la conclusion de cet examen était que, bien que certains progrès ont été accomplis (des progrès plus importants ont été constatés dans certains domaines), la gestion des risques au sein du MDN/des FC en était encore à une étape de développement relativement précoce lorsque cet examen a été effectué. Par la suite, des documents publiés par le MDN/les FC en octobre 2005 ont semblé être une réponse à certaines critiques contenues dans l'examen du CS Ex.

L'examen minutieux de ces documents suscite certaines préoccupations en ce qui concerne l'interopérabilité future au sein de divers éléments du MDN/des FC. D'importantes observations résultant de l'examen de ces documents portent à croire qu'au moins deux cultures distinctes sont présentes au sein du MDN/des FC en ce qui a trait à la gestion des risques. Plus particulièrement, la culture de risques opérationnels et celle du soutien des opérations du QGDN peuvent être difficiles à harmoniser. Cet examen a également confirmé les préoccupations du CS Ex en ce qui a trait au besoin d'une définition commune de la gestion des risques qui comprend l'utilisation actuelle. De plus, il existe une possibilité de rupture entre les approches de gestion des risques explicites et les approches implicites susceptibles d'être utilisées dans une situation réelle comportant un risque ou une menace. En outre, de plus récents documents (2005) mettent encore en évidence un aspect opérationnel distinct de la gestion des risques qu'il pourrait être difficile d'harmoniser avec les autres cultures présentes au sein du MDN/des FC, et encore moins avec d'autres organisations externes. Bien sûr, ce ne sont là que des observations préliminaires, mais elles indiquent un besoin de recherches plus approfondies en ce qui concerne ces problèmes.

D'autres articles ont été examinés en vue d'étudier l'interopérabilité potentielle du MDN/des FC lorsqu'ils sont en relation avec d'autres ministères comme Sécurité publique et Protection civile

Canada (SPPCC) et Santé Canada. Par exemple, des rapports du vérificateur général ont montré que les progrès accomplis par d'autres ministères quant au travail relatif à la gestion intégrée des risques étaient plutôt lents (2003) et que même les ministères particuliers chargés de la protection civile n'avaient pas établi une chaîne de commandement claire, n'avaient pas de normes et de pratiques communes et qu'ils n'étaient même pas interopérables dans leurs travaux de tous les jours (2005). Ces problèmes sont susceptibles d'avoir un effet dissuasif important relativement aux efforts en matière de gestion des risques.

Cela porte à croire qu'il reste encore beaucoup à faire pour aider les organisations à pratiquer la gestion intégrée des risques. Toutefois, il est également crucial que le gouvernement du Canada (et, aux fins de cet examen, le MDN/les FC) ne soit pas trop confiant en croyant que l'interopérabilité est assurée, même si chaque organisme gouvernemental a une excellente approche autonome de gestion des risques.

Le dernier chapitre de ce rapport décrit une approche de recherche qui étudierait la gestion des risques au sein du MDN/des FC de même que lorsqu'ils sont en relation avec d'autres organismes gouvernementaux susceptibles de prendre part à la réaction à des menaces terroristes en ayant pour objectif d'améliorer l'interopérabilité. Pour terminer, ce rapport décrit l'élaboration de questionnaires de recherche qui pourraient être utilisés pour examiner plus en détail ces problèmes, et il présente les questions qui pourraient être utilisées au cours d'entrevues directes. D'autres approches de recherche possibles sont aussi examinées, notamment l'élaboration de scénarios de gestion des risques. Espérons que ces recherches futures aideront à cerner les domaines où la gestion des risques pourrait être plus interopérable.

# Table of Contents

# List of Figures

# List of Tables

# 1. Introduction to Risk Management

## 1.1 Background

This project is in support of the Joint Command Decision Support for the 21st Century Technology Development Project. An important focus of this project is to understand how to improve the interoperability of defence- and security-related practices. Given that risk management is a critical factor in effective defence and security matters, understanding the extent to which risk management procedures are likely to be interoperable among government departments and departments is of great importance. Examination of the risk management procedures of Canadian Government departments contributes to the objective of the Joint Command Decision Support for the 21st Century Technology Development Project because these departments play a pivotal role in monitoring and responding to asymmetric threat.

Several trends have influenced the need to focus on risk management. In the aftermath of September 11th, 2001, the necessity of interagency cooperation in response to terrorist attacks has also been increasingly emphasized. New York City's response to the attack on the World Trade Centres involved fire-fighters, police, medical teams, national guardsman, and relief organizations. Countries across the world, including Canada, deployed a number of emergency crews to aid in relief efforts. Similarly, the March 11th, 2004 Madrid train bombings and July 7th, 2005 London public-transit bombings required the cooperation of many different departments in the rescue and relief efforts. Investigations into the September 11th terrorist attacks have revealed that intelligence communication failures between the Central Intelligence Agency and the Federal Bureau of Investigation were partly responsible for the government's inability to prevent the attacks (Johnson, Locy, & Kiely, 2003).

Since 9/11, there is increased recognition that Canada may be required to plan for, and possibly respond to, asymmetric threats such as terrorist attacks. The Canadian Security Intelligence Service (CSIS) states that "with the possible exception of the United States, there are more international terrorist organizations active in Canada than anywhere in the world" (CSIS, 2002), including Hezbollah, Hamas, and Jihad groups with possible links to Al-Qaeda. Al-Qaeda has listed Canada as one of five possible target countries; Canada and Italy are the only two countries that have yet to face an al-Qaeda attack (CTV.ca News Staff, July 8, 2005). Chief of Defence Staff, General Hillier, has publicly admitted that Canada is a potential terrorist target (CTV.ca News Staff, July 11, 2005).

In Canada, a potential terrorist attack would likely require the response of many different government departments. Public Security and Emergency Preparedness Canada (PSEPC), for example, might be responsible for ensuring that citizens are properly prepared and that they know what steps to take if a terrorist threat is detected. Health Canada might be responsible for planning for the potential health effects on Canadian citizens. The Royal Canadian Mounted Police (RCMP) may be involved in creating profiles of the potential perpetrators, and the Canadian Security Intelligence Service (CSIS) in gathering the intelligence that might help to prevent the attack. If these many systems do not have shared intent about their own role and responsibilities, if they assess the threat differently, or if they have no coordinated plan about how to manage the potential risk of a terrorist attack, Canada's response could be inadequate. Given the need for government departments to join together to manage crises such as terrorism events, it is critical to ensure that there is some level of consistency in how these different departments view risk management, and in

the risk management plans that they create. Clearly, government departments need to cooperate amongst themselves as well as with a range of other Non-Governmental Organizations (NGOs) to detect and to respond to terrorist threats wherever they occur. As such, it is important to ensure that effective risk management procedures are in place, and that these procedures are interoperable across government departments.

Indeed, in recent years, increasing the interoperability – or degree of coordination – among joint, interagency and multinational elements has been a priority of the Department of National Defence and the Canadian Forces (DND/CF). Newly emphasized constructs such as Effects-Based Operations and the Whole of Government approach promote the notion that the theatre of operations is much broader than previously envisioned, and that it is critical to look beyond conventional war-fighting depictions of the battle space. The joint, interagency, multinational, and public (JIMP) framework reflects the awareness that crises and conflict situations require complex responses involving military forces working in collaboration with other government departments (OGDs) and NGOs. Indeed, the CF's current operations in Afghanistan show a complex approach to providing humanitarian assistance while fighting the Taliban and working to stabilize a dangerous environment. This multifaceted approach requires coordination within the CF, as well as with OGDs and NGOs. Responding to potential terrorist attacks on Canada will require the ability to work across organizational boundaries to manage risk. In the scope of risk management that addresses asymmetric threats, this coordination would take the form of bringing together inter-organizational information on terrorist groups, putting together teams of counter-terrorism agents, coordinating emergency personnel and rescue crews, and communicating with the public to assuage fear. Given that many of the human-made as well as natural disasters for which Canada must prepare would most likely involve the United States, there would also be a need to coordinate response features to crises at a multinational level.

The Canadian government has been working for several years to ensure that potential threats are identified and that departments such as the DND/CF have a coherent plan in place to manage such threats if they occur. The resulting framework document, created by the Treasury Board of Canada Secretariat (2001), mandated that all Canadian government departments undertake a long-term process of building their risk management capability and establishing policies and procedures that would support an Integrated Risk Management Framework (IRMF). This report examines this standard and considers the progress made by the DND/CF in preparing to manage risk.

## 1.2 Purpose

The primary goal of this report is to highlight the risk management policies within the DND/CF in order to understand the extent to which this organization is likely to be interoperable with OGDs if and when required, as in the case of a terrorist threat.

Addressing this goal required reviewing the available standards regarding risk management to understand the degree to which government departments required to respond to asymmetric threats (such as terrorist attacks) are likely to be interoperable. Given the issues identified in the available literature, work was also undertaken to assist future research gathering data and exploring the risk management problem more fully. This consisted of developing a risk management survey to be used in future research. This survey would help to examine the way in which risk management procedures are likely to be interoperable, both within the DND/CF as well as across other government departments. Of specific interest for future research are PSEPC and Health Canada, due to the pivotal role they are likely to play in the Canadian government's response to a terrorist threat.

## 1.3 Structure of the Report

The report is structured into five sections. The current section provides the background and purpose of this project.

The second section will provide an overview of the concept of risk management as well as outline the various risk management standards and frameworks (e.g., Canadian Standards Association; CSA) that provide normative guides for what risk management procedures should entail. These standards will be used as a benchmark to evaluate the available risk management procedures of the DND/CF.

The third section discusses the available literature describing the DND/CF approach to risk management, and the potential challenges to interoperability that should be explored in more detail in future work.

The fourth section considers two possible approaches to understanding DND/CF interoperability in the event of a terrorist attack. This includes assessing interoperability within the DND/CF as well as in relation to other departments such as Health Canada and PSEPC. Critical issues to be addressed in assessing risk management interoperability are identified.

The fifth and final section provides a detailed account of the research tools created for future work exploring risk management within the DND/CF and in other relevant government departments, considers specific issues to be addressed in future research, and ends with a discussion of some of the challenges likely to be faced.


This page intentionally left blank.

# 2. Risk management Standards

## 2.1 Introduction and Definition

Risk management can be defined as the "systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues," with the aim of identifying significant risks and ensuring that "appropriate action is taken to minimize these risk as much as is reasonably achievable" (CSA, 1997, p. 2). The goal of risk management is to assist organizations to handle risks both within and external to the organization. Risk management policies allow organizations to set strategic priorities, and to anticipate and reduce risk, thereby increasing an organization's chance of success in achieving its goals and maximizing its ability to benefit from its activities.

A literature review was conducted in order to acquire information on (1) national and international standards for risk management, (2) the risk management procedures of the DND/CF, and (3) the extent to which the risk management procedures of the DND/CF reflect an Integrated Risk Management Framework (IRMF).

## 2.2 Treasury Board of Canada Secretariat - Integrated Risk Management Framework

The Canadian Government's formal approach to risk management (Figure 1) has emerged over several years, as shown in a report from the Office of the Auditor General of Canada (2003) exploring integrated risk management in several government departments.

| | |
|---|---|
| April 1994 | Risk Management Policy revised |
| October 1997 | *Report on the Modernization of Comptrollership* published |
| April 1999 | Treasury Board Secretariat's *Best Practices in Risk Management: Private and Public Sectors* |
| March 2000 | *Results for Canadians* report published |
| March 2000 | Privy Council Office's *Risk Management for Canada and Canadians*—Report of the ADM Working Group on Risk Management |
| April 2001 | Integrated Risk Management Framework published |
| April 2001 | *A Foundation for Developing Risk Management Learning Strategies in the Public Service* published by the Canadian Centre for Management Development Round Table on Risk Management |
| September 2001 | Implementation Council for the Integrated Risk Management Framework established |
| December 2001 | Inventory of federal risk management tools and departmental training |
| July 2002 | Treasury Board Secretariat's risk management Web site established |
| August 2002 | Modern comptrollership, which includes risk management, identified as a corporate priority by the Clerk of the Privy Council |

**Figure 1. Canadian government's risk management timeline (Office of the Auditor General of Canada, 2003, p. 5)**

The seminal event in this timeline was a document published by the Treasury Board of Canada Secretariat in 2001. This IRMF document was published as a guide to help government departments improve common priority setting and strategic planning related to risk management. The guide also aims to improve government employees' ability to anticipate, assess, and manage risk. The framework is set out to honour four commitments: citizen focus, values, results, and responsible public spending.

The purpose of the framework was to provide guidance for a systematic corporate risk management approach, to promote a risk-smart workforce and environment, and to provide risk management practices that departments can adopt. The IRMF was designed to support the government's governance responsibilities, improve results, strengthen accountability, and enhance stewardship. With the release of this document, other government departments were then expected to move forward with these broad risk management policies and practices and integrate them into their specific organizations.

Integrated risk management refers to the “continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective,” and is “about making strategic decisions that contribute to the achievement of an organization’s overall corporate objectives” (Treasury Board of Canada Secretariat, 2001, p. 7). It arises from the observation that it is no longer sufficient for risk to be managed at the individual and ‘functional silo’ level, wherein problems are addressed in isolation by only a few people. The IRMF emphasizes consultation and communication with stakeholders and the public, with the aim of minimizing losses and negative outcomes and identifying opportunities to improve services to stakeholders and the public at large. The Treasury Board of Canada Secretariat acknowledges that risk management is most rigorously pursued by departments involved with public health, public safety, and environmental protection, but there is also a need for increased risk management in other policy areas.

Several key processes at the centre of the risk management process were identified, and included developing the corporate risk profile, establishing an integrated risk management function, practicing integrated risk management, and ensuring continuous risk management learning. To develop the corporate risk profile, an environmental scan is conducted to identify both internal and external threats. Attributes of these risks are clarified, including its type, source, what is at risk, and the organization’s ability to control risk factors. The scan also identifies stakeholders’ and the organization’s tolerance of various levels of risk. Additionally, the scan assesses the internal risk management capacity of the organization, taking into consideration individual, group, organizational, and external factors.

Establishing an integrated risk management function involves the establishment of a corporate infrastructure that helps to provide risk management direction, integrating risk management into existing structures, and continuously building risk management capacity. This process involves establishing a clear statement of the organization’s commitment to risk management, incorporating risk management within organizational objectives and existing decision-making and feedback systems, developing a risk management-friendly corporate culture, and focusing on growing risk management capacity in human resources and tools and processes areas.

Practicing integrated risk management aims to consistently apply risk management principles at all organizational levels, to integrate results from risk management into decision-making and priority setting, to apply risk management tools and methods in decision-making, and to conduct ongoing internal and external communication with stakeholders. This is dependent on the use of a common, continuous model , drawn from the integrated risk management process as illustrated in Figure 2. This process stresses having a consistent risk management approach within an organization to allow aggregation of information.

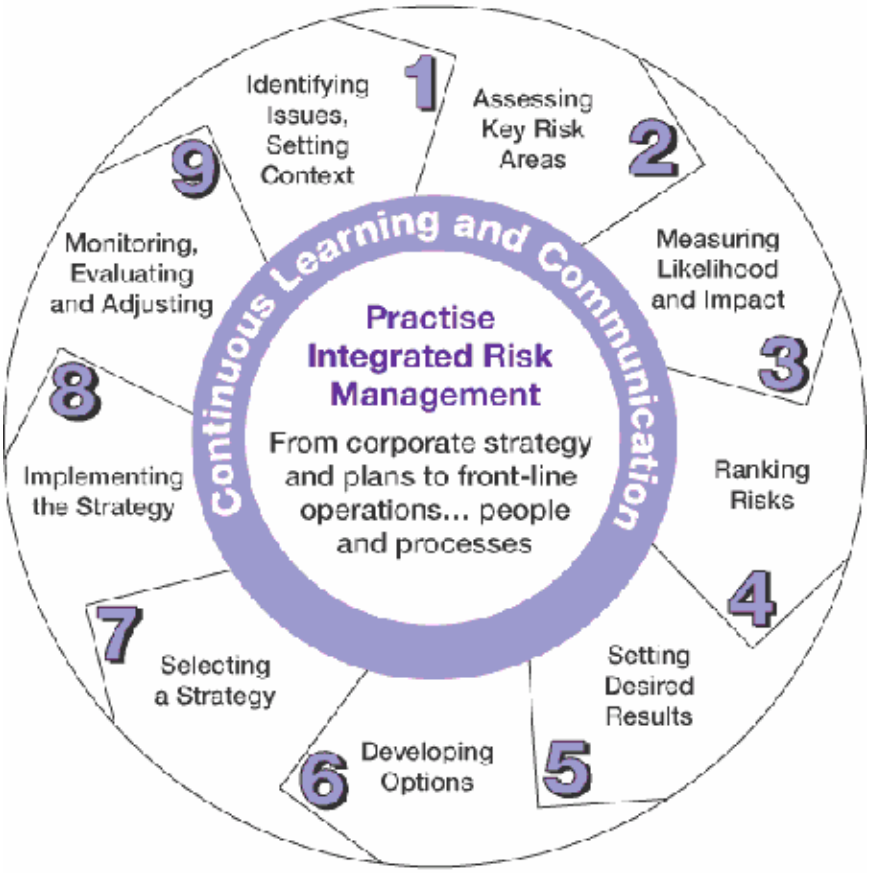


**Figure 2. Treasury Board of Canada Secretariat risk management model (2001, p. 15).**

The fourth element of the IRMF is continuous risk management learning. This framework aims to create a supportive, motivating work environment where employees can apply new learning and where management can demonstrate leadership. In addition, it focuses on integrating learning plans that identify the needs of each employee. Finally, results from risk management are evaluated to support further improvement.

The Treasury Board of Canada Secretariat's framework for risk management is also reflected in a companion document, the Integrated Risk management Implementation Guide (Treasury Board of Canada Secretariat, 2004), which provides more specific advice for organizations about how to actually implement the IRMF.

This broad approach to risk management was mandated by the Canadian government for implementation within all government departments, once tailored to meet the specific requirements of each government department. As will be discussed later in this report, there is some evidence that this implementation has occurred in some departments, whereas others seem to have made slower progress. The goal of this project, however, is to work to understand the extent to which organizations in the Canadian government (with a focus on the DND/CF) have made progress in this regard, and the extent to which they are likely to be interoperable with other departments in case of an asymmetric threat.

## 2.3 Canadian Standards Association (CSA)

The (CSA) is a non-profit organization that serves business, industry, government and consumers in Canada. The mandate of this organization is to provide standards that enhance public safety, safeguard health, promote trade, and protect the environment.

While the IRMF documents published by the Treasury Board of Canada Secretariat (2001; 2004) defines standards for departments within the Canadian government, risk management standards created by the CSA (1997) provide more generic standards that could be applied in any setting. The CSA identifies three dimensions of risk: frequency, or how often a loss might occur; consequence, or how large might the loss be; and perception, or how the potential risk is viewed by affected stakeholders. This document outlines a "comprehensive decision process that will aid decision-makers in identifying, analyzing, evaluating, and controlling all types of risks, including risks to health and safety" (CSA, 1997, p. 2).

The CSA Standard document offers a general model of managing risk with six stages, including initiation, preliminary analysis, risk estimation, risk evaluation, risk control, and action/monitoring, as shown in Figure 3.

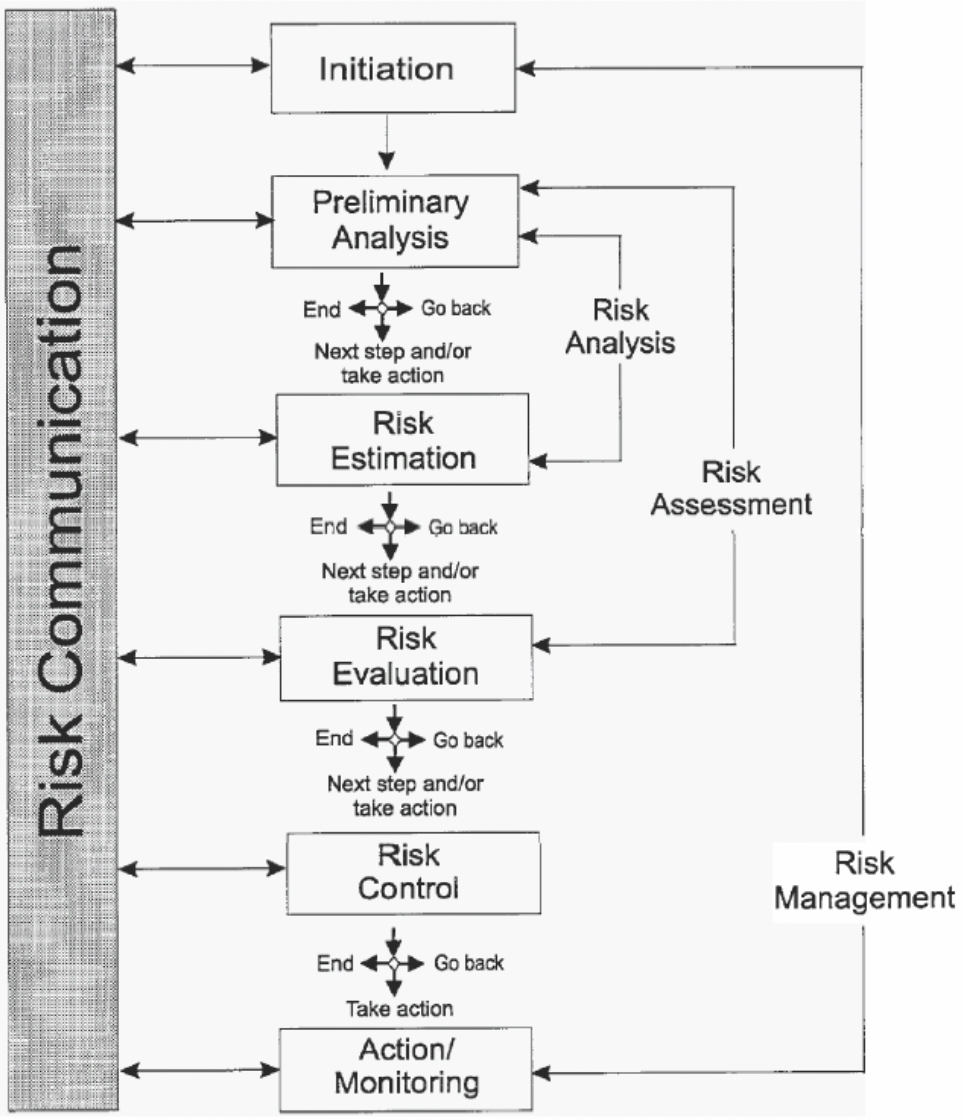


**Figure 3. Risk management model (CSA, 1997, p. 6)**

The CSA (1997) emphasizes that communication with stakeholders is critical at all stages of this process, with the goal of building trust, supporting effective and shared decision-making, reducing misperceptions, and improving the understanding of risk. The model also emphasizes that communication should not be only one-way from decision-maker to stakeholder; rather, it should consist of mutual dialogue. The CSA standard stresses that effectively and explicitly discussing uncertainties with stakeholders involved in risk estimates actually enhances a decision-maker's credibility. Because establishing and maintaining credibility is an important goal in risk communication, the CSA recommends training in risk communication prior to beginning risk management. The CSA standard also emphasizes documentation at all stages, and emphasizes the need to demonstrate accountability and due diligence.

The initiation stage consists of several administrative tasks to be completed by decision-makers. First, problems facing the organization are identified through discussion of key issues. Decision-makers bring together a skilled, multidisciplinary risk management team and assign them responsibilities and the authority required to accomplish their objectives. In addition, potential stakeholders, or "anyone who can affect, is affected by, or believes he/she might be affected by, a decision or activity (CSA, 1997, p. 12)" are identified.

Following initiation, preliminary analysis involves defining and evaluating the dimensions of the risk and building-risk scenarios to identify hazards that could generate potential losses. The risk management team also begins a stakeholder analysis to identify stakeholders and their needs, issues, and concerns. Information acquired to make risk management decisions is collected into a structured risk-information library. At the end of this stage a decision is made, such that the risk management team finds that a situation exists that requires immediate action, that there is a need for more detailed analysis before any action, or that the risk is not of immediate concern.

If the decision is that immediate action is required, the next stage is initiated. The risk-estimation stage focuses on defining methods that will be used for the analysis of risk scenarios. These methods can include statistical models, historical data or professional judgment. A formal third party is introduced to review and validate these planned analyses. At this stage, the risk management team also needs to estimate the frequency and consequences of risk scenarios, and to update the stakeholder analysis through dialogue with stakeholders.

The risk management team then proceeds to risk evaluation, where the acceptability of the risk is considered in relation to the needs, issues, perceptions, and concerns of the stakeholders. The team also identifies the direct and indirect costs and benefits associated with potentially risky issues. The CSA guideline suggests that risk management teams try to reduce the risk as much is reasonably possible (CSA, 1997). At the end of this stage, the risk management team comes to a conclusion as to whether the risk is unacceptable, acceptable, or acceptable but requiring risk-control measures.

If the risk management team decides that the risk needs to be reduced via risk control, then risk management proceeds to the next stage. In the risk-control stage, the risk management team anticipates the level of risk that would exist before and after potential controls are implemented. The team also analyses the costs, benefits, and risks of the control options and any residual risks, which must be financed either by the organization or by insurance. Possible risk-control measures include: avoiding exposure to risk, reducing the frequency and the consequences of the loss, separating exposures, duplicating assets, and transferring obligations (e.g., through insurance). During this process, the best control strategy is defined as the one that costs the least, reduces losses the most, and has the least-adverse side effects.

At the final stage of risk management, action/monitoring, the team designs and implements the selected risk-control options. Following implementation, the risk management team establishes a monitoring process that works to detect and adapt to changing circumstances, to monitor progress, to ensure that strategies are properly implemented, and to verify assumptions made throughout the risk management analyses.

This guideline provides a relatively comprehensive list of the necessary considerations in initiating a risk management process. The risk management process is presented in a general way as to be applicable to a wide variety of organizations, and it provides a broad overview of the issues at the early stages of developing a risk management system.

## 2.4 Other International Standards

### 2.4.1 United Kingdom Institute of Risk Management - A Risk management Standard

Another risk management 'best practices' standard prevalent in Europe was created by three major risk management organizations in the United Kingdom - The Association of Insurance and Risk Managers (AIRMIC), the Association of Local Authority Risk Managers (ALARM), and the Institute of Risk Management (IRM). The National Forum for Risk Management in the Public Sector co-published these risk management guidelines (AIRMIC, ALARM, & IRM, 2002), outlining risk management best practices against which organizations can measure themselves. Importantly, the guideline states that different organizations should approach the key components of the standard in different ways, and that the standard should not be seen as a prescriptive, universal risk management method. The document classifies risks as coming from external and internal factors, as shown in Figure 4.

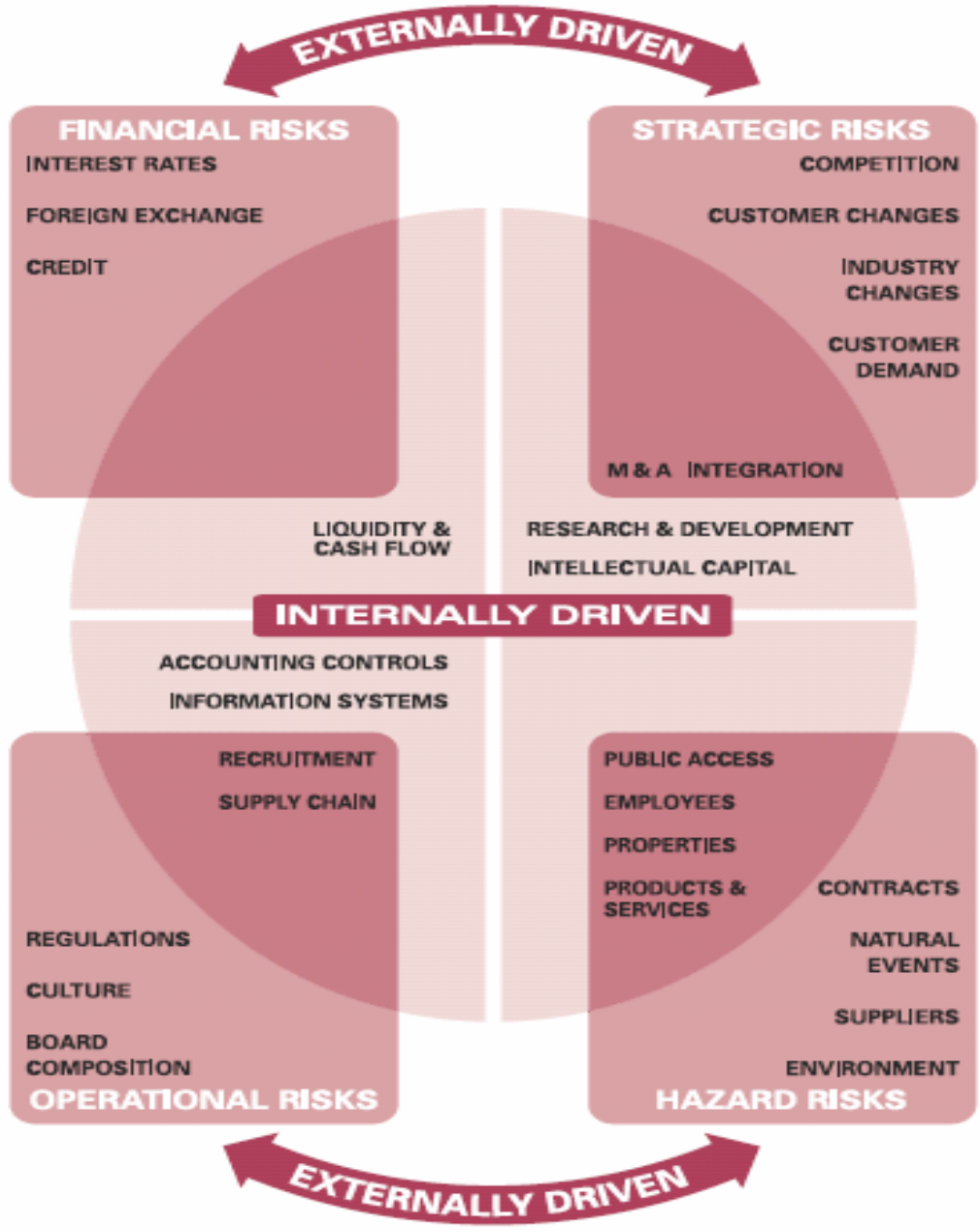


**Figure 4. Examples of the drivers of key risks (AIRMIC, ALARM, & IRM, 2002, p. 3)**

This figure includes risks from within the organization as well as external to it. There are many external risks, including financial, strategic, operational, and hazard risks, as well as risks that intersect internal and external domains. It is important to note that this standard also frames risk in a broader context, "Risk management should be a continuous and developing process which runs throughout the organization's strategy and the implementation of that strategy….It must be integrated into the culture of the organization with an effective policy and a programme led by the most senior management." (AIRMIC, ALARM, & IRM, 2002, p. 2).

Overall, the standard suggests that risk management should support the organization's strategic objectives by providing a consistent and controlled framework for future activity, improving decision-making, planning, prioritization, resource allocation, efficiency and company image, protecting assets, reducing volatility, and supporting an organization's personnel and knowledge base. A diagram of this risk management process is illustrated in Figure 5.

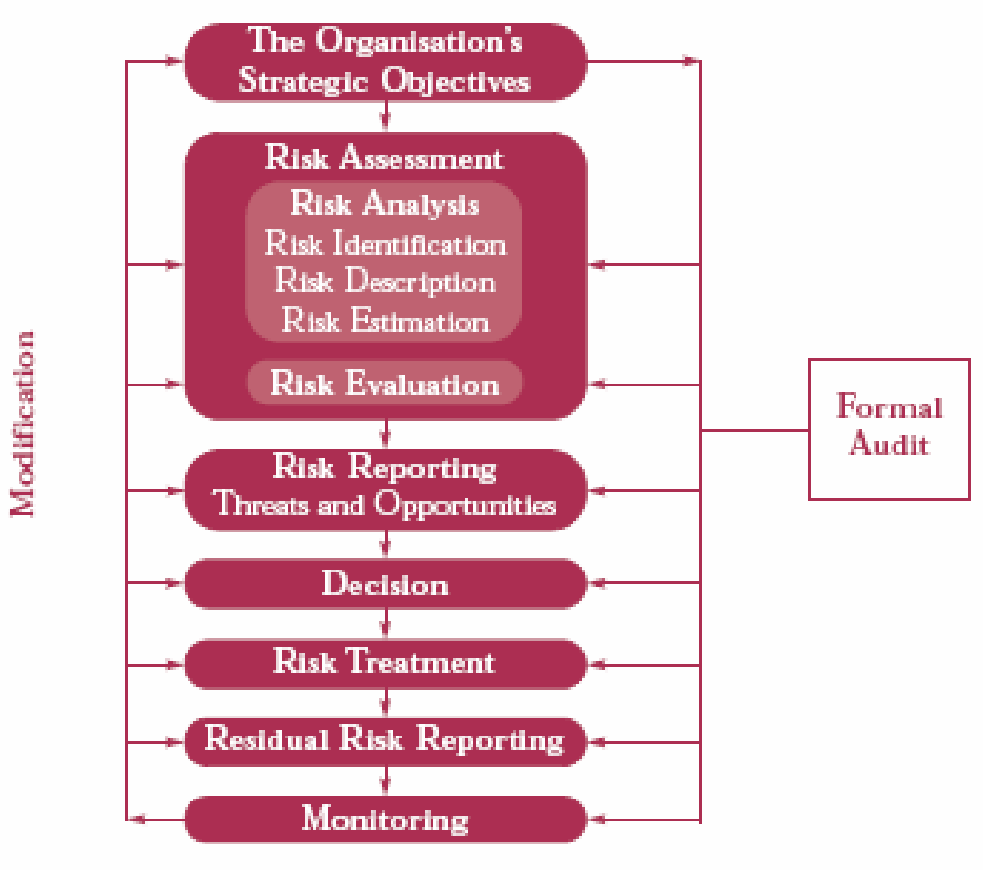


**Figure 5. United Kingdom risk management process (AIRMIC, ALARM, & IRM, 2002, p. 4)**

This risk management process starts with risk assessment, a procedure comprised of risk analysis and evaluation. The document recommended a variety of risk-analysis methods for both upside risks (opportunities) and downside risks (threats; see Annex A). These methods produce a risk profile that allows for the rating and prioritization of risk treatments, and the mapping of risks to different business areas where ownership of risk is recognized. This inclusion of both opportunities and threats in risk management is an important one. It seems apt that the goal of proper risk management is not only the prevention of adverse events, but also recognition of the risks of missing opportunities that could benefit the organization.

Risk analysis consists of three components: identification, description, and estimation. Risk identification requires understanding the organization and its objectives, its market, and relevant legal, social, cultural, and political environments. The report suggests that risk from organizational activities and decisions may be classified into strategic, operational, financial, knowledge management, and compliance categories (Table 1).

**Table 1. Nature of risk (AIRMIC, ALARM, & IRM, 2002, p. 4)**

| Nature of Risk | Definition |
|---|---|
| Strategic | Long term objectives that are affected by changes in capital, politics, legal issues and regulations, reputation and physical environment. |
| Operational | Day-to-day issues in achieving strategic objectives. |
| Financial | Managing organizational finances, influenced by credit, foreign exchange and interest rates, and market exposure. |
| Knowledge Management | Management, production, and communication of knowledge; influenced by external factors of intellectual property issues, area power failures, competitive technology; internal factors of system malfunction and staff loss. |
| Compliance | Health and safety, environmental, trade, consumer, and regulatory issues. |

Risk-identification methods include brainstorming, questionnaires, business studies, industry benchmarking, scenario analysis, workshops, incident investigations, auditing, and inspections. In risk description, risks are displayed in a structured table (Figure 6) that allows for the comprehensive identification, description, assessment, and prioritization of risks.

| | |
|---|---|
| 1. Name of Risk | |
| 2. Scope of Risk | Qualitative description of the events, their size, type, number and dependencies |
| 3. Nature of Risk | Eg. strategic, operational, financial, knowledge or compliance |
| 4. Stakeholders | Stakeholders and their expectations |
| 5. Quantification of Risk | Significance and Probability |
| 6. Risk Tolerance/ Appetite | Loss potential and financial impact of risk<br>Value at risk<br>Probability and size of potential losses/gains<br>Objective(s) for control of the risk and desired level of performance |
| 7. Risk Treatment & Control Mechanisms | Primary means by which the risk is currently managed<br>Levels of confidence in existing control<br>Identification of protocols for monitoring and review |
| 8. Potential Action for Improvement | Recommendations to reduce risk |
| 9. Strategy and Policy Developments | Identification of function responsible for developing strategy and policy |

**Figure 6. Structured table for risk description (AIRMIC, ALARM, & IRM, 2002, p.6)**

Risk estimation can take place in qualitative or quantitative form, depending on the type of organization involved (see Annex B).

The second part of risk assessment, risk evaluation, is the comparison of estimated risks against an organization's risk criteria to determine their relative significance and necessity for risk reduction. An organization's risk criteria may include issues such as cost and benefits, and legal, socio-economic, environmental, and stakeholder concerns.

Following risk assessment, the organization moves onto risk reporting. Internally, different levels in the organization are generally responsible for relevant activities that require the awareness or production of risk information (Table 2).

**Table 2. Internal reporting tasks (AIRMIC, ALARM, & IRM, 2002, p. 9)**

| Organization Level | Task |
|---|---|
| Board of Directors | Know significant risks facing the organization |
| | Know the effects on shareholder value of deviations from expected performance |
| | Ensure appropriate risk management awareness throughout organization |
| | Know how the organization will manage a crisis |
| | Know the importance of stakeholder confidence |
| | Manage communications with investors |
| | Be assured that risk management is working effectively |
| | Publish a clear risk management policy |
| Business Units | Be aware of risks in their area of responsibility and its relations to other areas |
| | Have performance indicators that monitor key activities, objectives and required interventions |
| | Have systems which appropriately communicates variances in budgets and forecasts |
| | Report systematically and promptly to senior management about risk management developments |
| Individuals | Understand accountability for individual risks |
| | Understand how they can enable continuous risk management improvement |
| | Understand that risk management and risk awareness are part of organizational culture |
| | Report systematically and promptly to senior management about risk management developments |

Clearly, at all levels of the organization, specific units each play a role in ensuring that risk communication and reporting occur.

Externally, an organization needs to regularly report its risk management efforts to its stakeholders, providing information about finance, community affairs, human rights, employment practices, health and safety, and the environment. The reports also need to address risk management responsibilities, risk-identification procedures, risk management controls, and risk management monitoring and review systems. These formal, external reports should be made readily available to stakeholders. The risk-report stage allows the organization to come to a decision about how to approach risk treatment.

Risk treatment is "the process of selecting and implementing measures to modify the risk" (AIRMIC, ALARM, & IRM, 2002). It includes the control/mitigation, avoidance, and transfer of risk. The organization must also consider their ability to fund the financial consequences of risk. A good risk-treatment system should provide effective and efficient organizational operation, effective internal controls, and observe legal and regulatory compliance. Management must prioritize controls for risks identified during the risk-analysis process, and these controls need to be evaluated in terms of their costs and benefits, and the consequence and cost of no action must also be considered in the analysis.

A monitoring-and-review process is included to ensure that appropriate controls are in place and that procedures are understood and followed. Such a process includes regular policy and standards compliance audits and performance reviews, and should also account for changes within the organization and its environment. The standard insists that allocation of resources and responsibilities to enable risk management within an organization need to be clearly established. This stage also helps to determine whether the assigned controls have worked as intended, whether the assessments made were appropriate, and identifies lessons learned.

The standard also provides guidance on the administration of risk management. An organization's stated risk management policy should describe its approach to and appetite for risk. It also needs to clarify its organizational responsibilities, referring to legal and regulatory requirements where necessary. A strong risk management policy requires management commitment, clear assignment of responsibilities, and proper resource allocation. Specifically, the Board of Directors (or other management team) must determine the organization's strategic direction and create an environment where risk management can operate effectively. It needs to take into account the nature, extent, and likelihood of acceptable risks, how to manage unacceptable risks, the company's ability to manage the risks, the cost and benefits of the risks and the control activity, the effectiveness of the risk management process, and the risk implications of management decisions. Business units are responsible for risk management on a day-to-day basis, for promoting risk awareness in operations, for introducing risk management objectives, and for ensuring that risk management is incorporated at all project stages.

Depending on the size of the organization, risk management may be handled by a part-time or full-time risk champion, or a full-scale risk management department. This person or team is responsible for setting risk management policy and strategy, championing risk management at strategic and operational levels, building a risk-aware culture, establishing internal business-unit risk policy and structure, designing and reviewing risk management processes, co-ordinating risk management functional activities within the organization, developing risk-response processes, and preparing risk reports.

Furthermore, independent, objective internal audits help to monitor significant risks within an organization. These audits provide assessments of current risk management policies and active support and involvement in the risk management process. They also facilitate risk identification,

assessment, and reporting. In addition, the audits play a role in educating staff about risk management.

Risk management needs to be embedded in an organization's strategic and budget processes, as well as in training, development, and operational processes. This standard explicitly states that, although risk identification can be facilitated by external consultants, actual 'in-house ownership' of risk management processes is critical, as risk management must be (and be seen to be) a central part of the strategic management of the organization. This emphasis seems consistent with the Treasury Board of Canada Secretariat's (2001) guidelines' insistence on risk management processes being fully integrated into the everyday processes of an organization.

### 2.4.2 Australian/New Zealand Standards for Risk Management

One of the most current risk management standards is co-published by Standards Australia and Standards New Zealand (2004). Similar to the Canadian Standard (CSA, 1997), this is a generic standard, independent of specific industry employed, and is intended to be utilized according to the varying needs of an organization. The stated objective of this standard is to help organizations to achieve a more confident and rigorous basis for decision-making and planning, better identification of opportunities and threats, gain value from uncertainty and variability, manage risk proactively, effectively allocate resources, improve incident management, reduce the costs of risks, improve stakeholder confidence and trust, improve legislative compliance, and improve corporate governance. Risk management is defined as "the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects" (Standards Australia and Standards New Zealand, 2004, p. 6), and risk management principles can be applied at the strategic, tactical, and operational levels of an organization.

As in other models, one of the main elements of the risk management process is communication and consultation involving dialogue with internal and external stakeholders. Stakeholders' perceptions of risk need to be identified and incorporated into the decision-making process. The standard emphasizes a consultative approach, instead of one-way information flowing from decision makers to other stakeholders. This bidirectional communication approach allows appropriate definition of the context to ensure risks are identified, and can encompass diversity in expertise and points of view. In addition, it promotes ownership of risk - the appreciation of the benefits of risk controls and the need to endorse risk management.

The risk management process as specified by these standards is very similar to the other standards already described (Figure 7).

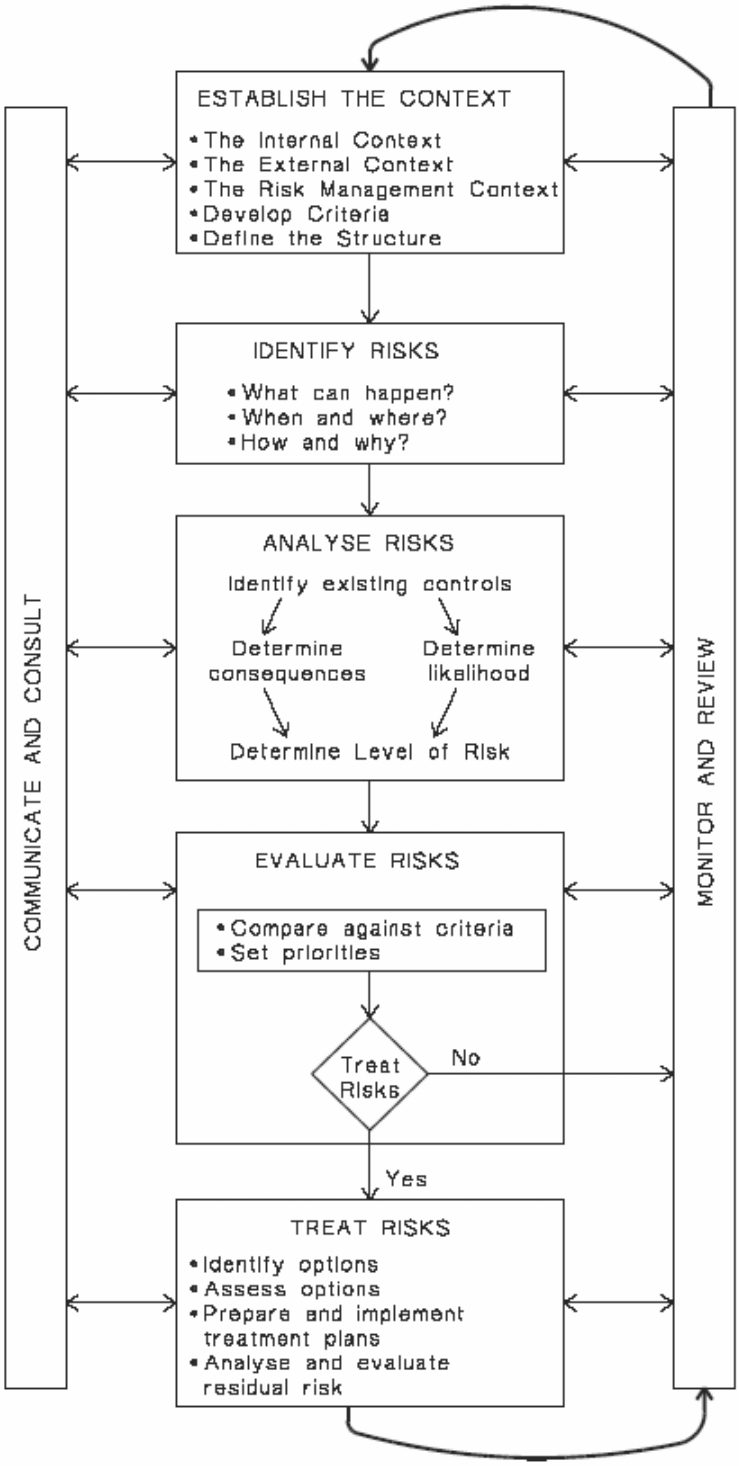


**Figure 7. Standards Australia and Standards New Zealand (2004, p. 9) risk management process overview**

The Standards Australia and Standards New Zealand (2004) publication divides risk management into several components. First, the risk management process needs to take into account the organization's relationship with its external environment. This could include the business or regulatory environment, and also includes the strengths and weaknesses of the organization. The risk management process also needs to take external stakeholders into account and establish communication with them. The internal context of risk management also needs to be considered. Internal context includes the organizational culture, structure and objectives, internal stakeholders, and organizational capabilities. Furthermore, the risk management context is established by defining organizational activities, decisions to be made, the temporal and geographical extent of organizational activity, the depth of risk management to be carried out, and identifying studies that need to be conducted. Based on these contextual factors, risk criteria are developed, and should be further refined throughout the risk management process. This culminates in a structured logical framework of activities for the organization's risk management process.

The risk management process proceeds to the task of risk identification. This involves generating a comprehensive list of sources of risks and events that can impact organizational objectives identified in the contextual stage. It involves examining when, where, and how these risks could be encountered using various techniques such as checklists, judgements based on experience and records, systems analysis, and systems-engineering techniques.

Risk analysis considers how risks should be treated and the specific approaches required. This involves considering the sources of risks, positive and negative consequences, and the probability of these consequences. In addition, existing controls need to be analyzed. Analytical methods to determine consequences and likelihoods can be based on statistical analysis or on subjective estimates such as past records, experience, published literature, market research, models and expert advice.

### 2.4.3 Overview of Risk management Standards

Analysis of the national and international standards on risk management shows many similarities and areas of overlap among the different standards. One of the most prominent elements common among the various standards is the notion of a continuous risk management process, whereby feedback loops exist to ensure the best possible results. Most standards also stress the importance of an integrated framework, such that risk management becomes an integral part of business function, strategic objectives, and organizational culture, rather than being a disembodied process occurring within an isolated group. Within an integrated framework, risk management is more likely to be viewed as a critical means of achieving organizational objectives.

Similarly, the standards emphasize the need for multiple roles and responsibilities in the management of risk. That is, risk management must be handled by diverse individuals (in terms of levels and function) throughout the organization rather than by a select few people.

The importance placed on stakeholder communication and involvement is another key aspect of the risk management process in both the national and international standards. Such communication should occur throughout all stages of this process, with the goals of building trust, sharing decision-making, and improving the understanding of risk. The authors of the standards also tend to agree that communication should not be one-way from decision-maker to stakeholder; rather, it should consist of mutual dialogue to facilitate accurate risk assessment and to maintain credibility between the organization and its stakeholders. As well, it is important to remember that the inclusion of both

opportunities and threats in risk management is important, as missed positive opportunities can also impede organizational progress.

Overall, the large degree of overlap in terminology and approaches between these different risk management standards suggests that there is widespread agreement in the basics of how risk management should be conducted. However, these standards are very general, and it remains the responsibility of an organization to decide how to bring these into actual practice, and the conversion of basic risk management principles into practice is likely to be influenced by both organizational expertise and culture.

The next section explores DND/CF efforts to bring these risk management guidelines into formalized policy and practice.

This page intentionally left blank.

# 3. Interoperability of Risk Management within the Department of National Defence and the Canadian Forces (DND/CF)

The need to coordinate efforts when managing risk is evident between and within organizations. There are many diverse groups and elements within the DND/CF that may be required to work together to manage a crisis, and they all share the same goal. “The fundamental goal of the DND and the CF is to protect Canada, and Canadian interests and values, while contributing to international peace and security” (DND, n. d.) The ability for the various elements of the DND/CF to be truly interoperable would depend on the risk management procedures and strategies they are likely to initiate when external threats present themselves. As such, it is important to understand the current approach of the DND/CF to risk management. Interoperability issues become more difficult once other organizations become involved, as they may have different goals which also must be considered.

## 3.1 Key Documents Addressing Risk Management in the Department of National Defence and the Canadian Forces (DND/CF)

In attempting to understand the risk management practices and culture in the DND/CF, there are several available sources of information. The first is a document which presents doctrine related to risk management procedures to be used during the operational planning process (DND, 2002). Another document reports the results of a study exploring the progress that the DND/CF had made in implementing its own version of the Treasury Board of Canada Secretariat’s (2001) mandated risk management plan (CRS & Deloitte & Touche, 2004). Finally, two recent documents have been issued by the DND/CF, the Integrated Risk management Guidelines (DND, 2005a) and the Integrated Risk management Policy (DND, 2005b), which appear to address the shortcomings identified by the CRS and Deloitte & Touche baseline review. Each of these is reviewed in the following sections.

### 3.1.1 Joint Doctrine Manual: Risk Management for Canadian Forces (CF) Operations

The Joint Doctrine Manual: Risk Management for CF Operations (DND, 2002) seems to represent one part of the DND/CF response to the federal government’s mandate that all government departments should have a risk management strategy.

This manual states that the goal of CF risk management is to “enhance operational capabilities and mission accomplishment, with minimal acceptable loss” (DND, 2002, p. 1-1). The manual aims to provide operational planners with a simple, consistent template to examine risk and decision processes in identifying, analyzing, evaluating and controlling all types of risk. Tools provided are intended to ensure that significant risks are identified and that appropriate action is balanced against operational objectives to ensure that risks are minimized. This document acknowledges the need for planners to speak from a common base, corresponding to the interoperability theme. The goal in conducting risk management is to perform the least amount of risk assessment necessary to clearly identify critical threats and permit courses of action (COA) to be compared and risk

acceptance decisions to be made. The CF risk management plan is closely linked to the phases of the CF operational-planning process.

This document defines risk management as “a process that assists decision makers in determining how to reduce or offset risk and to make informed decisions that weigh risks against mission benefits,” that must be “integrated into the planning, preparation, and execution of operations” (DND, 2002, p. 1-1). Within this manual, risk is defined as “an expression of a possible loss or negative mission impact stated in terms of probability and severity of an event” (p. 1-1). The CF uses risk management to assist decision makers to determine how to reduce or offset risk, and to weigh those risks against mission benefits in order to identify the optimal course of action.

The manual identifies two main risks in military planning. Tactical risks involve threats that exist because of the presence of an enemy or party to a conflict capable of violent acts. It applies to all levels of war and across the spectrum of conflict. Accident risk refers to all other risk considerations, such as friendly operations, civilian activities, equipment readiness, health and environmental issues. This document also presents the idea that, in modern conflicts, accident risks often exceed tactical risks.

DND (2002) presents risk management as the commander’s responsibility, and stresses that risk management must be fully integrated into the planning, preparation and execution of operations. Risk management is useful in generating, training, deploying, and employing a task force, because it enhances decision-making skills, provides improved confidence in the task force’s capabilities, and protects personnel and equipment by avoiding unnecessary risk. The techniques used in the manual mirror the United States services’ techniques to promote interoperability. However, the risk management process is not intended to replace operational decision making, nor can it remove risk completely.

The DND (2002) document outlines four principles for risk management. First, commanders should accept no unnecessary risk, and only accept the level of risk required to complete the task. Second, making risk decisions at the appropriate level is critical, and commanders must ensure that subordinates know how much risk they can accept and when to elevate the risk decision to a higher level. Third, risks should be accepted when their potential benefits outweigh their potential costs. Fourth, risk is best managed by anticipation and planning.

DND (2002) also points out that the CF faces two types of planning environments. A ‘crisis action’ environment applies during the execution phases of training or operations; it is an ‘on-the-run’ mental or verbal review of the situation using an abbreviated version of the basic risk management process. ‘Deliberate’ planning takes place when time is not critical. Here, group experience and brainstorming sessions help identify threats and develop controls. Deliberate planning is used for planning upcoming operations, reviewing standard operating procedures, maintenance, training, and developing damage or disaster response plans. These planning environments, presumably, can also be described as proactive and reactive.

The DND/CF conceptualization of a continuous risk management process is shown in Figure 8. It is quite similar to the other standards reviewed here. The DND (2002) document stresses a balance in resource allocation to each step of the risk management process. Furthermore, the process should be applied in sequence, and as a cycle – the entire risk management process is circular to accommodate additional threats and the impact of risk management actions.

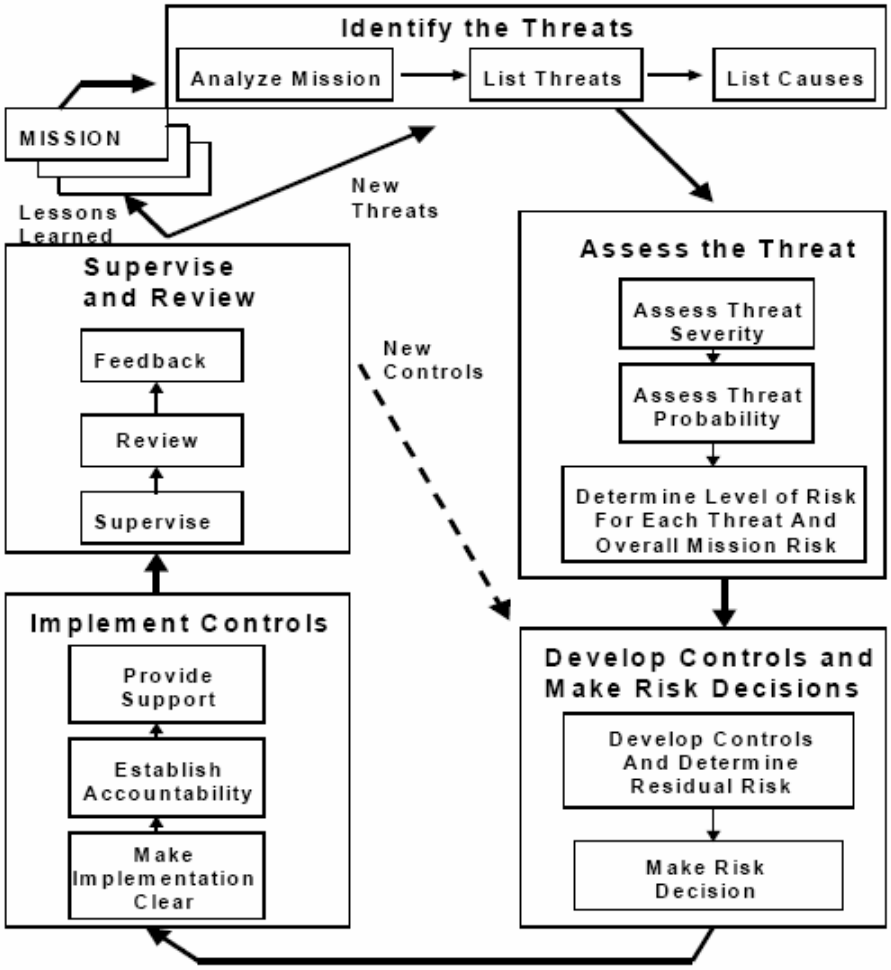


**Figure 8. Continuous application of risk management (DND, 2002, p. 2 – 4)**

DND (2002) describes risk management in terms of two primary activities, risk assessment and risk mitigation.[1] The risk assessment activity begins with identifying threats, and examines threats associated with mission degradation, personal injury or death, and property damage. In the process of identifying threats, it is necessary to analyze the mission by breaking it down into 'bite-size' chunks. In addition, all possible threats and causes of such threats must be listed. Threat assessment includes assessing the probability and severity of threats and using a risk-assessment matrix to prioritize the threats (Figure 9).

[1] Risk communication is noted, but is not discussed in this manual because the manual is purported to address the operational-planning process. As such, it is implied that risk communication is less critical.

| Risk Assessment Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | | Probability | | | | |
| Severity | | Frequent A | Likely B | Occasional C | Seldom D | Unlikely E |
| Catastrophic | I | E | E | H | H | M |
| Critical | II | E | H | H | M | L |
| Marginal | III | H | M | M | L | L |
| Negligible | IV | M | L | L | L | L |

(E - Extremely High Risk; H - High Risk; M - Moderate Risk; L - Low Risk)

**Figure 9. Risk-assessment matrix (DND, 2002, p. 3-2)**

Pitfalls to be avoided during the risk management process in risk assessment include over-optimism, misrepresentation of perspectives, alarmism (i.e. improbable worst-case estimates), indiscrimination toward weighting data, subjectivity and/or hidden agendas, bad or misunderstood data, and the inappropriate quantification of human behaviour. DND (2002) recommends that commanders avoid complex analysis techniques, especially those in engineering design, that involve an enormous amount of calculations.

The risk-mitigation activity involves developing controls, making risk decisions, implementing controls, and overseeing and reviewing the control implementation. A table of criteria for effective controls is presented in Figure 10.

| Criteria for Effective Controls | |
|---|---|
| Control Criteria | Remarks |
| **Suitability** | Control removes the threat or mitigates (reduces) the residual risk to an acceptable level. |
| **Feasibility** | Unit has the capability to implement the control. |
| **Acceptability** | Benefit gained by implementing the control justifies the cost in resources and time. |
| **Explicitness** | Clearly specifies who, what, where, when, why, and how each control is to be used. |
| **Support** | Adequate personnel, equipment, supplies, and facilities necessary to implement a suitable control are available. |
| **Standards** | Guidance and procedures for implementing a control are clear, practical, and<br>Specific. |
| **Training** | Knowledge and skills are adequate to implement a control. |
| **Leadership** | Leaders are ready, willing, and able to enforce standards required to implement a control. |
| **Individual** | Individual personnel are sufficiently self-disciplined to implement a control. |

**Figure 10. Criteria for effective controls (DND, 2002, p. 3-3)**

Controls may be classified into engineering (e.g., fire-control mechanisms for armoured vehicles), administrative (e.g., written policies), educational and training, physical (e.g., barriers or signs), and operational (e.g., rules of engagement) controls. These controls help by 1) avoiding risk by cancelling the task or operation, 2) delaying the risk by postponing the mission, 3) transferring the risk to another unit or platform, or assigning redundant capabilities to ensure that potential losses

can be compensated for. Controls are applied to the risk until the level of residual risk matches the commander's guidelines or cannot be further reduced. The commander alone must decide if controls are sufficient and acceptable and whether to accept the resulting residual risk. When implementing controls, there should be an emphasis on clear directives, personnel and resource support from higher command, as well as accountability for risk-control decisions.

Oversight and review of risk-control measures are used to determine the effectiveness of risk controls used throughout the operation. This involves determining whether controls are correctly and effectively in place and that required changes can be identified and implemented. Re-evaluation should take place any time personnel, equipment, or mission tasks change, or new operations are anticipated. The commander also needs to review whether the benefits of risk management are as helpful to mission performance as expected. And, at the end of the process, the commander needs to initiate 1) evaluations in the form of after-action reports, surveys, and in-progress reviews, and 2) a feedback system incorporating documentation, briefings, lessons learned, benchmarking or database reports.

The risk management doctrine also stipulates how risk management should be incorporated into the CF operational-planning process, as shown in Figure 11. The manual outlines specific procedures required at each stage of the CF operations-planning process.

| Risk Management in CF Operational Planning | | | | | | |
|---|---|---|---|---|---|---|
| | | Identify Threats | Assess Threats | Develop Controls Make Risk Decisions | Implement Controls | Supervise And Review |
| CFOPP | Stage I Initiation | X | | | | |
| | Stage II Orientation | X | X | | | |
| | Stage III COA Development | X | X | X | | |
| | Stage IV Plan Development | | | X | X | |
| | Stage V Plan Review | | | | | X |
| Rehearsals | | | | | X | X |
| Employment and Assessment | | | | | X | X |

**Figure 11. Risk management phases and CF operations-planning process (DND, 2002, p. 3-6)**

During initiation, the commander, along with his staff, reviews the mission plan as well as possible threats. In the orientation stage, consideration is given to mission threats that are beyond the task force capabilities. These threats include enemy capabilities that may pose threats to the operation, terrain and weather, the capabilities of troops and support (e.g., emotional and physical health), time available and civilian considerations (e.g., civilian unrest).

During COA development, the commander and staff continue to identify threats and begin to develop controls to reduce their risk. Once COA are analyzed for feasibility and acceptability in terms of residual risk, the commander selects a preferred COA. Once the COA is approved, the

staff incorporates the controls into the mission through the development of a discrete plan. This plan is then reviewed to determine if the risk management process was applied correctly.

DND (2002) also explores the functions and responsibilities that need to be taken on by the staff. As found in the Treasury Board of Canada Secretariat (2001) document, this doctrine stresses that the risk management process has to be embedded into the CF operation, culture, organization, systems, and also into individual behaviour. Although risk management is guided by individual commanders, risk management must be supported by the chain of command and is also the responsibility of everyone in the chain of command (Figure 12).

| RISK MANAGEMENT RESPONSIBILITIES | |
|---|---|
| Commander | Provide Risk Guidance |
| | Select Control Options |
| | Make Risk Decision for COA |
| | Enforce and Evaluate Controls |
| Chief of Staff | Supervise Risk Management and Integration Across Entire Staff |
| | Ensure Threats and Controls are Integrated into Plans and Orders |
| | Ensure Staff Monitors Controls During Execution |
| Staff Officers (Functional Areas) | Identify Threats Most Likely to Result in the Loss of Combat Power |
| | Develop Control Options that Address Causes of Threats |
| | Integrate Threats and Selected Controls into Functional Area Paragraphs, Graphics, and Annexes of OP O and plans and Then Monitor Implementation During Execution |

**Figure 12. Risk management responsibilities (DND, 2002, p. 4-6)**

However, as Figure 12 shows, although risk management is intended to be performed at all levels, the commander is the single person who makes the risk decision about what COA to take. Specifically, the commander directs the command climate, and needs to display support of the risk management process. He or she must lead by example and:

- Provide clear guidance and feasible goals
- Obtain and provide assets required for risk management
- Understand capabilities and display confidence in his or her team
- Inform, consult and listen to subordinates
- Prevent a zero-defect mindset and allowing learning from mistakes
- Update planning as the mission changes
- Train, evaluate and supervise subordinates on the risk management process
- Assess the risk management process and disseminate lessons learned
- Display confidence in subordinates, informing, consulting and listening to subordinates
- Keep track of issues such as casualties, environmental damage, civilian loss, and public
- Empower leaders by pushing risk decisions as far down the chain of command as feasible within the next higher commander's guidance

The DND (2002) document states that the Chief of Staff is responsible for supervising the integration of risk management across the staff, and this involves coordinating controls that affect multiple functional areas and adjacent units. The staff is also required to assist the commander throughout the stages of the risk management process. In addition, commanders may also establish force-protection working groups as well in order to help assess and monitor threats. Each primary Joint Staff directorate (the co-ordinating headquarters for strategic and operational planning) is also assigned specific risk management responsibilities (see Annex C).

Finally, individual staff members are also responsible for risk management and should carry the practice over into both on- and off-duty activities. In theory, any staff member has the authority to halt something that is inherently unsafe. Inexperienced or complacent staff should beware of overconfidence and the underestimation of risks.

According to DND (2002), it is critical that commanders continually monitor "the complexity of mission development and associated changing relationships with other departments" (p. 4-7), as well as being respectful of cultural issues and sensitivities. Integration of risk management into the DND/CF and its operations involves considerations of the relationships between the DND/CF and other departments, civilian contractors, media, NGOs, private volunteer organizations, and local indigenous populations.

DND (2002) also mentions several problematic issues that are identified as needing to be overcome when doing risk management, including 1) commanders not wanting to recognize risk (risk-denial syndrome), 2) staff members who do not want to bother the commander about risk decisions, 3) subordinates who fail to understand guidance, and 4) failure to recognize threats and personnel overconfidence. Other identified threats to the risk management process include over-zealous 'zero defect' standards that often lead to organizational paralysis. Moreover, the doctrine also encourages leadership to take responsibility for errors.

It is also critical that the risk management process undergoes continual review, so that leaders understand the effectiveness of their risk management processes. This includes consideration of many different activities, including how well threats and controls are identified in oral and written communication, plans, and standard operating procedures; how well risks are communicated to the lowest level of command; whether risks are integrated into training plans; whether the consideration of risk is included in both on- and off-duty activities; whether the consideration of risk is embedded into force-protection programs; and whether the consideration of risk is included in after-action reviews and lessons learned. Although these points are raised, exactly how these processes should be enacted, unfortunately, is not specified in DND (2002).

### 3.1.2 Chief Review Services' (CRS's) Assessment of Risk Management in the Department of National Defence and the Canadian Forces (DND/CF)

The CRS is a part of National Defence. Its mandate is to perform reviews with the purpose of promoting improvements in the DND/CF and to enhance the DND/CF's ability to perform at the highest ethical standards (DND, n.d.). In January 2004, the CRS and Deloitte & Touche jointly conducted a baseline study assessing risk management policy in the DND/CF (CRS & Deloitte & Touche, 2004). This report assessed risk management policy with reference to both the IRMF and a five-stage risk management Maturity Model adapted from work by Deloitte & Touche. This model was used to assess the sophistication of current risk management practices used in the DND/CF and to identify areas for improvement.

To aid in this research, representatives from Level 1 organizations (e.g., Land Staff, Air Staff) attended work sessions and interviews to discuss integrated risk management practices and perceptions of risk information. Participants also completed a diagnostic tool developed for the research based on the four pillars of the IRMF (incorporated into Annex D). The tool included 24 'best practice' statements related to the four elements of integrated risk management (identifying important risks and priorities; establishing roles and responsibilities for risk management; applying an integrated risk management approach; enabling risk management and learning from experience). Participants anonymously rated their own experience against each best-practices statement and these ratings were used as a starting point for discussions (CRS & Deloitte & Touche, 2004).

Findings from the diagnostic tool and subsequent interviews indicate that the DND/CF, like other public sector organizations, had yet to fully embrace and bring integrated risk management into maturity. Key elements of the optimal integrated risk management process were compared with the DND/CF processes in place at the time of the report. Conclusions drawn from a comparison of these key elements identified a number of critical inadequacies in the DND/CF approach.

CRS and Deloitte & Touche (2004) did note that not all areas of the DND/CF lacked a risk management process, and some areas showed relatively sophisticated risk management process. Indeed, the military operational-planning process (as exemplified in DND (2002), reviewed earlier) was assessed as having a fairly good risk management process outlined and used within the Joint Staff Action Team. In other specific areas, risk management procedures were also farther along than in most of the DND/CF. For example, in areas related to financial management and environmental health and safety, risks were seen to be managed proactively with the use of formal or traditional methods. However, at an organizational level, the progress made in understanding operational risks did not appear to have carried over to the National Defence Headquarters' corporate culture or to operations support's culture. The review noted that risk management within the corporate environment was viewed as a normal part of conducting business and a routine managerial function. However, within the support function, internal client expectations and risk tolerances were generally not well communicated, and reward structures favoured results achieved rather than competence management of uncertainties. As such, the audit concluded that the necessary level of consistent formalization in risk management was lacking within the DND/CF. For instance, the report stated that "[a]lthough integrated risk management is already somewhat embedded in military operational activities, it is not evident in other DND/CF corporate and military support activities" (CRS & Deloitte & Touche, 2004, p. iii).

Communication was also identified as a problem, and the inadequacy of risk information sharing within the DND/CF was highlighted. Risk information was communicated on a "need-to-know basis to those in authority rather than shared" (CRS & Deloitte & Touche, 2004, p. 10). Furthermore, personnel seemed hesitant to reveal risk information in fear of receiving negative feedback and appearing to be incapable. They also seemed to be constrained by policies governing the exchange of classified information. As such, there was a commonly-held belief in certain groups that risks should only be communicated to senior management if a solution had already been found.

Risk identification within the DND/CF was also identified as a potential problem area, as it was sporadic rather than continuous and more reactive than proactive (see Figure 13).

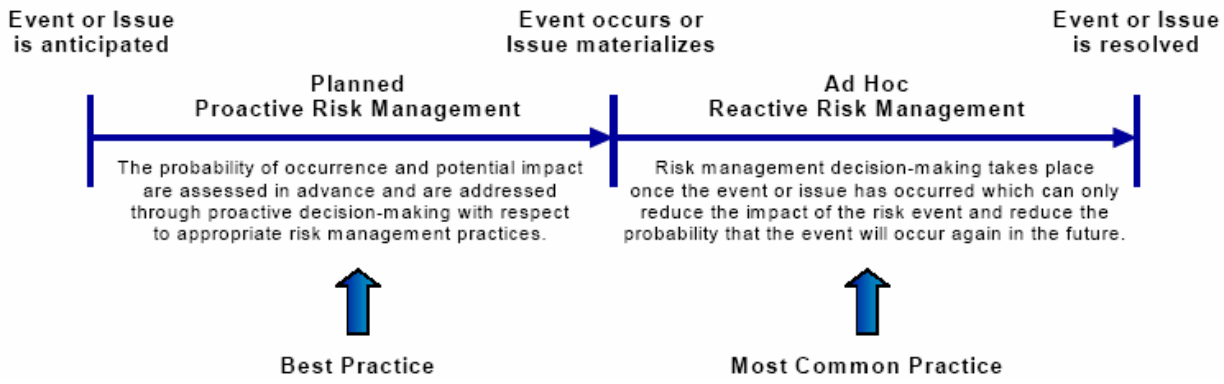


**Figure 13. Best practice vs. current state of the DND/CF (CRS & Deloitte & Touche, 2004, p. 11)**

The CRS and Deloitte & Touche (2004) review indicated that risk identification was often more intuitive than systematic, and not necessarily based on consistent, structured analysis where risks are ranked and compared. This document noted that the DND/CF business plans were generally lacking in risk management assessment. For example, although risk management was often used by Chiefs of Staff to identify specific risks, these were generally limited to assessing resource limitations and did not include other risks such as risks to infrastructure, risks to the goodwill of the local population, etc. Finally, risks were seen as sometimes purposely analyzed at low levels so that projects received approval. Environmental scanning of risks was not widely practiced within the DND/CF, leading to limited ability to foresee problems.

Risk identification in the DND/CF was reported to be assigned to managers rather than being seen as everyone's responsibility. This observation seems justified given the emphasis in CF doctrine on the commander as the primary 'risk manager' and others as having an (at least implicitly) subordinate role. This emphasis on leaders as the primary champions of risk management can prevent information about risk tolerances permeating through the entire organization.

Another critical requirement in responding optimally to risk is being able to identify individuals responsible for responding when risks are identified. The CRS and Deloitte & Touche (2004) report revealed that the DND/CF risk management roles and responsibilities were not clearly defined, not formalized, and often poorly understood. In particular, job responsibilities were not specific with respect to risk management, and assignment of risk ownership was not always clear in support or corporate functions. The report also noted that designated Offices of Principal Interest should exist in areas where risk is actively managed (e.g., financial management), but few currently provide specific support for risk management within the Level 1 (e.g. Land Staff, Air Force Staff) organisations. Finally, personnel in the operational context reported more comfort with the level of risk they are expected to manage than do personnel in the corporate environment.

As a whole, the CRS and Deloitte & Touche (2004) report found that there were no common risk management processes, and that definitions of risk and risk management were not widely understood, communicated, or applied across the DND/CF. In fact, military and civilian staffs defined risk differently, and risk management practices across the DND/CF differed significantly from location to location. And, although the Deputy Chief of Defence Staff had drafted a risk management framework for CF operations, it had not been fully implemented. Furthermore, information to identify and assess risks did not always exist. The report also found that there was

little understanding of risk and risk management consistent with the Treasury Board Secretariat's IRMF, and also little understanding of the necessity for integrating risk management into the regular day-to-day function of the DND/CF. Accordingly, the report noted that "a management infrastructure that includes common risk language, information elements, reporting guidelines and technology is not yet in place to enable widespread deployment of integrated risk management" (CRS & Deloitte & Touche, 2004, p. 18). In addition, there was no consistent reporting of risk information to senior management (or even a way for senior management to seek such information) and no system for documenting and communicating lessons learned.

In order to assess the level of integrated risk management within the DND/CF, comparisons were made to the risk management maturity continuum (Figure 14).

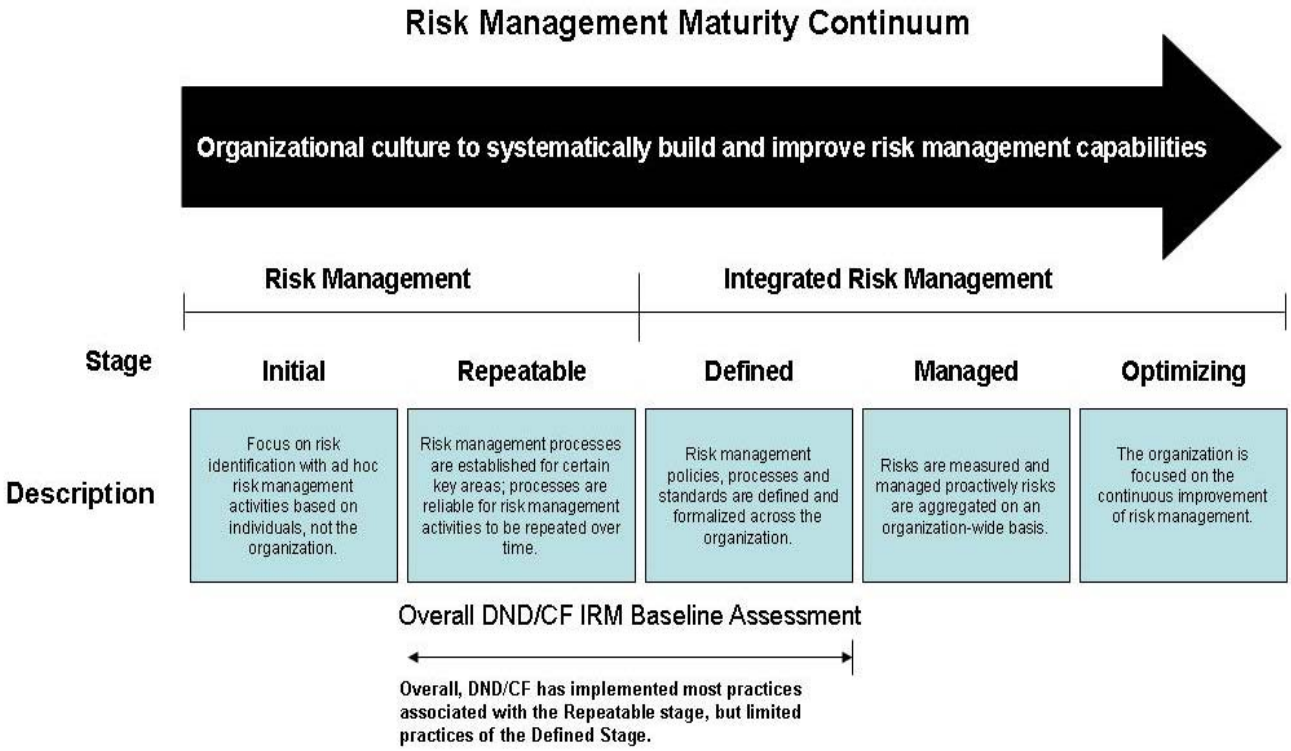


**Figure 14. Maturity continuum (DND, 2002, p. 4-6)**

This graphic illustrates the procession of an organization through the different stages of risk management, from initial considerations (still wholly lacking integration), to a middle phase in which an organization is starting to define stable processes and procedures that are more consistent over time, to a final, more integrated system that is formalized and which becomes an integral part of the organizational culture.

Overall it was found that the DND/CF had implemented most of the practices associated with the Repeatable stage and showed a limited number in the Defined stage, placing the DND/CF in a middle phase of the risk management maturity continuum. Further, although some areas within the DND/CF were shown to manage risk at the Managed and Optimizing stages, such progress was

isolated and inconsistent. Given such evidence, it appears that although effective risk management was in place in certain areas of the DND/CF as of 2004, the organization had not taken enough steps to fully adopt the Treasury Board of Canada Secretariat's (2001) IRMF, and did not have a continuous, proactive and systematic process to understand, manage and communicate risk on an organization-wide basis. Some of the specific discrepancies noted are shown in Figure 15.

| IRM Key Element/Characteristic | THE DND/CF Comparison (Generally) |
|---|---|
| Continuous, dynamic risk identification as early warning | Relatively sporadic & annual identification |
| Possible risk events proactively identified before occurrence | Largely reactive to risk event occurring |
| Systematic Process in place | Risks considered principally as they relate to business planning |
| Structured analysis of likelihood & impact | Mainly intuitive analyses, although pockets where structure used |
| Everyone identifies risks | Mostly a manager's responsibility to identify risks |
| Organization-wide process | Process not yet in place |
| Risk managed at lowest practical level | Risk tolerances often not known or communicated; therefore, difficult for lower levels to manage risks |
| Risks prioritized | Unstructured prioritization |
| Reporting of prioritized risks upwards | Reporting partially through annual business planning |
| Mitigation plans commensurate with severity & likelihood or risks | Few mitigation plans based on risk assessment |
| Open communication of risks | Limited horizontal communication |

**Figure 15. Comparison of the DND/CF with ideal integrated risk management elements (CRS & Deloitte & Touche, 2004, p. 12/28)**

The barriers to integrated risk management implementation identified by the CRS and Deloitte & Touche (2004) included a lack of support from senior management, a lack of department-wide policy, and scepticism about the benefits of risk management. In addition, the report criticised the existence of a DND/CF organizational culture where risks are not fully disclosed for fear of weakening a proposal, where risk disclosure is associated with bad news and poor performance, where risk information is not readily shared horizontally, and where there is worry that risk information will be exploited to criticise the organization. Two of the primary needs indicated in the report were having a risk management 'champion' within the organization and having a full risk profile.. In general, risk management was not recognized as a necessary foundation for an ethical climate by the DND/CF. Key issues required to address the identified barriers within the DND/CF included:

- "Fostering a culture receptive to innovation, prudent experimentation and responsible risk taking;
- Providing adequate resources to establish a framework for integrated risk management;
- Developing a flexible departmental risk management framework to allow for customization and Level 1 priorities;
- Scanning for external influences and changing priorities in order to ensure risk information remains current and relevant;

- Developing classification guidelines for the protection of sensitive risk-information" (CRS & Deloitte & Touche, 2004, p. 22).

The review made six recommendations to the Vice-Chief of Defence Staff (VCDS; the current VCDS is Lieutenant-General W.J. Natynczyk). The VCDS should: serve as a high-level risk management champion, develop an overarching departmental IRMF for the CF (Figure 15) and a long-term integrated risk management implementation plan. The VCDS should also coordinate Level 1 organizations and develop a corporate risk profile. Finally, he or she should be responsible for developing risk-communication strategies, for initiating risk-awareness training, and for promoting open risk communication. These actions on the part of the DND/CF were likely to bring them to a more advanced stage of an integrated risk management approach, as shown in Figure 16.

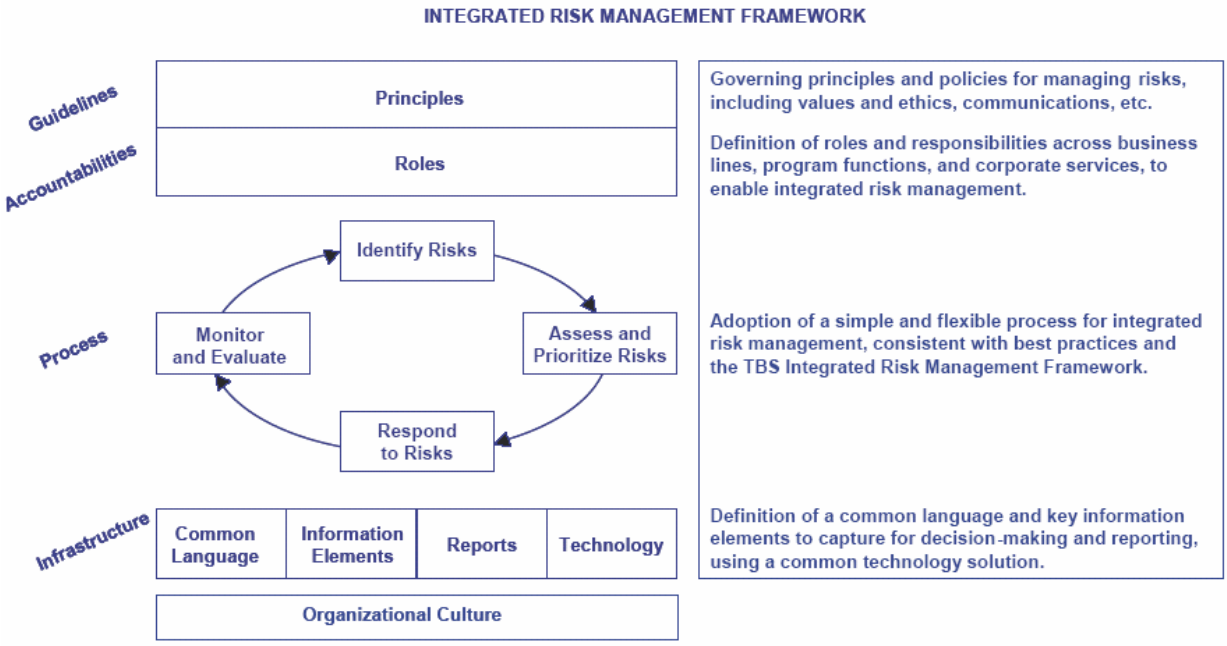


**Figure 16. Integrated Risk Management Framework (CRS & Deloitte & Touche, 2004, p. VII)**

These documents laid out the optimal risk management procedures that should be used by the DND/ CF. If properly implemented, they should allow maximal levels of interoperability and the ability to coordinate risk management procedures across diverse organizations.

In general, this report was both critical of the DND/CF in terms of its need to move forward more aggressively toward a full integration of risk management into the organization and organizational culture, and sympathetic in noting the potential inertia of moving a large and diverse organization toward such a complex organizational change. It was noted that the DND/CF had made some effort, but was still at the early stages of articulating a fully integrated risk management approach.

### 3.1.3 Department of National Defence and Canadian Forces (DND/CF) Integrated Risk Management Policy and Guidelines

In an effort to address the issues brought forward by the CRS and Deloitte & Touche (2004), the DND/CF released two new documents that outlined the guidelines and policies of an IRMF to be

used throughout the DND/CF. These documents were drafted to allow the DND/CF to proactively, systematically and explicitly manage risk, thus supporting informed decision making and strategic objectives. The first document defines the integrated risk management policy that the CF and Department will use (DND, 2005b), and the integrated risk management guidelines outline "IRM [integrated risk management] methodology and provides a suite of tools for the consistent application of risk management" (DND, 2005a, p. 1).

At a policy level, the first document clearly shows recognition of the need to address the different cultures in the DND/CF, and to have a single IRMF guiding the organization. It also recognizes the need for a common method and terminology to be used throughout the DND/CF. This document (2005b) identifies the VCDS as the 'facilitator' of the risk management process, as lessons learned are used to refine practices. The 'operational risk profile' is defined as the means by which an integrated process will emerge, and the depiction of integrated risk management from the CRS and Deloitte & Touche (2004) report is also used in this document. The operational risk profile used to "provide the guidance needed for middle and senior management to make the choices necessary to attain defence objectives consistently" (DND, 2005b, p. 5). The Chief of Defence Staff and Defence Minister are identified as the people required to "review the Corporate Risk Profile on a regular basis" (DND, 2005b, p. 6).

The DND/CF Policy report on risk management (DND, 2005b) also outlines responsibilities of key parties within the DND as they relate to the deployment and ongoing use of integrated risk management. Lastly, this document identifies the need to communicate this policy throughout the DND/CF, and to ensure better communication of risks, both horizontally and vertically.

The more elaborated integrated risk management guidelines (DND, 2005b) work to further elucidate the DND/CF approach to promulgating risk management. The DND/CF approach needs to be generic and not tied to a specific function or organizational level (e.g. strategic, tactical etc.) within the DND/CF. This document then works to specify:

- Risk management methodology
- Infrastructure requirements, tools and techniques
- Communication approach

Each of these areas is then addressed in more detail.

Risk management Methodology - The risk management process is described in the DND/CF guidelines on risk management (DND, 2005a). The risk management process is broken down into four distinct stages: identify; assess and prioritize; respond; and monitor and evaluate. The guidelines outline several steps involved in risk identification: (1) identify mission/objective that may be at risk; (2) decide on necessary people, tools and techniques; (3) consider possible causes of risk; (4) define the problems or opportunities, scope, context and associated risk; (5) perform a stakeholder analysis, including risk tolerances, stakeholder position and attitudes; and (6) identify the risk owner and degree of control over the risk. Risk identification can occur through a workshop in which key members and stakeholders brainstorm possible short and long term risks and devise a comprehensive list of risk areas. However, this document does not articulate who the stakeholders might be.

Having identified the risks, the next step is to assess which risks are the most serious based on qualitative measures of likelihood of occurrence (ranging from 1 = rare to 5 = almost certain) and a qualitative measure of the impact of such occurrences (ranging from insignificant to severe), as shown in Figure 17.

| Impact | Mission Success | Financial ($) | Health & Safety | Environmental Protection | Reputation | Legal |
|---|---|---|---|---|---|---|
| **5 Severe**<br><br>Would stop achievement of functional goals/ objectives | Fail to achieve mission objectives | Suggest remove $$ figures<br><br>$10-$100M<br><br>> 25% | Multiple fatalities, or significant irreversible effects to >50 persons | Very serious, long-term environmental impairment of ecosystem functions | Significant loss of client group trust<br><br>Public outcry for removal of Minister and key officials | Could have an adverse national impact on national defence and security, fed-provincial relations, law enforcement, public health & safety |
| **4 Major**<br><br>Would threaten functional objectives | Some mission objectives at risk, overall marginal effective-ness | $1-$10M<br><br>16 to 25% | Single fatality and/or severe irreversible disability<br><br>(>30%) to one or more persons | | Serious public or media outcry (international coverage)<br><br>Severe criticism by review agencies | |
| **3 Moderate**<br><br>Necessitates significant adjustment to overall function | Mission achieved with day-to-day crisis issues. Supporting tasks at risk | $100K-$1M<br><br>6 to 15% | Moderate irreversible disability or impairment (<30%) to one or more persons | Serious medium term environmental effects | Adverse national media/public/NGO attention<br><br>Criticism by OAG, TBS.<br><br>Some loss of client group trust | Adverse impact on DND/CF policy or operations<br><br>Could impose costs on DND/CF in excess of budgeted funds |
| **2 Minor**<br><br>Would threaten an element of the function | Most objectives met | $10K-$100K<br><br>2 to 5% | Objective but reversible disability requiring hospitalization | Moderate, short-term effects but not affecting ecosystem functions | Attention from media and/or local community. Criticism by NGOs | Minor legal issues, non-compliances and breaches or regulation |
| **1 Insignificant**<br><br>Lower consequences/ impact | Mission achieved with minor shortfalls | <$10K<br><br>< 2% | First aid treatment | Minor effects on biological or physical environment | Some unfavorable media attention<br><br>Setback in building of client trust | Disclosure of personal information with minor impact |

**Figure 17. Qualitative measures of impact (DND, 2005a, p. 6)**

Each risk is assigned Likelihood and Impact ratings which are mapped onto a grid to determine the overall threat to the objectives. This map or grid is intended to assist decision making "as it

identifies the risks that need to be managed actively based on their threat to accomplishment of the mission" (DND, 2005b, p. 7).

Having determined the overall risk inherent in the situation, a risk response needs to be developed. The response involves developing a plan to reduce the likelihood of the risk's occurrence and to minimize the impact should it occur. For a plan to be developed, leadership must either determine the threshold that risks must reach to require a response or decide on a maximum number of risks that can be managed on a daily basis. There are four main risk-response strategies:

1. Avoid – the task/activity/project is cancelled;
2. Transfer – risk is transferred horizontally or escalated to a more appropriate level within the organization;
3. Accept – either develop a contingency plan or do nothing until the risk occurs and then react;
4. Mitigate – action is taken prior to the risk occurring to reduce the likelihood of occurrence or the impact.

Ideally, risk responses should be created in low-stress environments, and plans should be created for all risks above the threshold set by the leadership. In determining the risk response, one should consider the desired results or expected outcomes from the risks; develop options in dealing with the risk; select an option based on residual risk and the assessment of cost against the benefits; and finally, plan and implement the option.

Risk monitoring and evaluation forms a continuous loop with risk identification and analysis. Questions that need to be answered at the monitoring and evaluation stage include: 'Were the responses effective and timely?' and 'Were they accurately assessed from a cost and performance perspective?'. This report also provides a link to a VCDS website which will act as a repository of lessons learned and best practices in risk management.[2] This provides a response to criticisms in the CRS and Deloitte & Touche (2004) review about the need to have a clear mechanism within the DND/CF to learn from past mistakes.

Infrastructure – An explicit philosophy of the work in this policy document is to create an integrated risk management process that minimizes additional process. At the most basic level, important elements of infrastructure are common terminology, technology, and reporting process. The terminology used in the report is consistent with that from the Treasury Board of Canada Secretariat's (2001) report. Technology would leverage existing capability and would be eventually linked to business planning, performance measurement, and other management applications. No additional technology is seen as necessary, other than ensuring that the reporting process is sound. The reporting process is described in fairly simple terms, and the need for it to occur both formally and informally (as well as often) is indicated. With regard to the reporting process, the guidelines state that communication is important to the integrated risk management effort and will occur formally and informally. Overall, it is critical to collect and deliver clear, accurate, timely, and relevant risk information. The creation of 'templates' is also indicated so that risks can be identified, tracked and reported in a sample risk log.

Communication - Finally, communication is a necessary element in the adoption of an IRMF. Integrated risk management involves two dimensions: (1) communicating the policy to strengthen

[2] Unfortunately, this link is no longer active and an updated link could not be found.

the implementation of integrated risk management throughout the organization, and (2) improving communication of risk horizontally and vertically. In addition, the DND/CF guidelines staff and stakeholders should be engaged well in advance of the possible realization of a risk,

Lastly, some general principles of risk communications are presented, including

- Be prepared – engage communications staff appropriately
- Some risks will require a proactive response
- Some risks will require a reactive response
- An appropriate risk communications response is situational, but will be based on the Government of Canada policy and the Treasury Board of Canada Secretariat's (2001) risk-communication approach

These two documents, then, form the available written record of the DND/CF response to the review undertaken by the CRS and Deloitte & Touche (2004). At a broad level, DND (2005a) and DND (2005b) show the intention of the DND/CF to be responsive to the Treasury Board of Canada Secretariat's (2001) document mandating increased attention to risk management procedures.

## 3.2 Potential Challenges to the Department of National Defence and Canadian Forces (DND/CF) Interoperability

The goal of this project was to provide information about the potential interoperability of the DND/CF and other government departments in the event of a major risk such as a terrorist attack. At this point, there is limited information on which to base this observation. The available documents, however, provide valuable insight into potential areas of focus for future work. Our observations of the written material show several areas in which the apparent lack of congruence has the potential to undermine interoperability.

A critical challenge to interoperability relates to the existence of unique risk management cultures within the DND/CF. The DND (2002) document outlining CF doctrine related to risk management is a good example of how personnel within the operational community see the risk management process. Having defined it solely in terms of the risks associated with a specific mission, this document adopts a valuable but constrained definition of the risk management process. At the most basic level, one of the most important messages of the CRS and Deloitte & Touche (2004) review was that even though the risk management approach within the DND/CF is still at an early stage of development, the lack of a unified risk management culture may pose problems when timely and efficient processes are required. The operational community is only one part of the larger DND/CF organization, and the Treasury Board of Canada Secretariat's (2001) approach mandates that government departments have one integrated process rather than separate procedures for different parts of the same organization. Even the 2005 reports (DND 2005a; 2005b) still show persistent (albeit perhaps unintentional) references to the distinctly operational culture rather than the National Defence Headquarters/operational support cultures. Indeed, the DND (2005a) report shows continued emphasis on thinking about risks based on "…their threat to accomplishment of the mission" (DND, 2005a, p. 7). As such, even though the DND/CF has indicated their intention to create a fully integrated risk management process, their own 2005 documents seem to indicate a risk management process that may not be fully integrated into the corporate structure. within the DND/CF.

There are several practical reasons why the different risk management cultures in the DND/CF may exist, and why it may be difficult to create a risk management strategy that is adequate for all areas

of the DND/CF. The nature of the risks (e.g., financial risks versus potential loss of life, including the life of the decision-maker), the amount of time available to make decisions (e.g., years versus seconds), and the availability of communication methods (e.g., free communication versus no or unsecured communications when on a mission) are at least three reasons why somewhat distinct risk management cultures may still exist. Put simply, it may be very difficult for the optimal risk management approaches to be equivalent when the challenges faced are so dissimilar. This suggests that being able to capture the nuances in how personnel from often divergent cultures understand risk management would be of critical importance in promoting maximal interoperability

The attitudes of the people within an organization are likely to be a critical predictor of the hurdles that might be faced when advancing integrated risk management. The CRS and Deloitte & Touche (2004) review had noted that senior management had not adequately embraced integrated risk management. Both the initial Treasury Board of Canada Secretariat's document and the CRS and Deloitte & Touche review talk of a truly integrated risk management process as being like 'a journey' for organizations.

> "IRM [integrated risk management] is often referred to as a journey, as it encourages changing the culture from one of risk aversion to one where risks are viewed as uncertain events that can contribute positively or negatively to the achievement of organizational objectives." (CRS & Deloitte & Touche, 2004, p. I).

Unfortunately, the DND (2005a; 2005b) documents do not provide a clear view of how positive risk management attitudes in the DND/CF actually are. However although these more recent DND/CF documents are closer to the ideas inherent in the CRS and Deloitte & Touche report, these documents continue to present a relatively legalistic and somewhat detached view of risk management. The spirit advocated in the Integrated Risk Management Framework report seems to be missing from these 2005 documents. To be fair, this could represent less than positive attitudes toward integrated risk management, or could simply represent a lack of familiarity and/or comfort with integrated risk management processes. However, achieving the most advanced level of maturity on the risk management continuum, and being interoperable with other departments will require full knowledge and acceptance of the concept of integrated risk management. If, within a given organization, written policy is simply a mandated response (e.g. to standards such as the Treasury Board of Canada Secretariat's; 2001) but is not actually used as such, it will be impossible for other departments to predict and interpret the reluctant organization's responses.

This suggests that assessing the congruence between the explicit policies and implicit attitudes and beliefs about risk management will be important in working toward promoting maximal interoperability within the DND/CF. Thus, it will be important to elicit the views of the DND/CF personnel in order to understand their beliefs, expectations, and attitudes toward risk management, and the dominant risk management culture within various departments. Hopefully, future work that will provide more richness and detail to the issues noted in this document review. The next chapter works to define possible elements of work more specifically.

Another critical factor that could influence interoperability relates to decisions about who should have responsibility for risk management within an organization. DND (2002) has the potential to undermine interoperability because it seems to constrain responsibility primarily to the operational commander. Persistent references to the commander described as the primary initiator and 'final word' in the risk management process, and the very hierarchical approach indicated in this document could arguably be at odds with the requirements of an integrated risk management approach in which an entire organization is implicated in identifying, assessing and responding to risk. This operational risk mentality (rather than the broader corporate risk mindset) is even evident

in the DND (2005a; 2005b) reports with their continued emphasis on the leader as the focal point of the risk management process. To be fair, the strongly hierarchical structure of the DND/CF is an integral part of the organization; thus, it must remain as part of their risk management strategy. However, care must be taken to stress to all members of the DND/CF that risk management is also their responsibility, and the responsibility of all members of the DND/CF must be made clear. As such, understanding how risk management roles and responsibilities are seen in varying departments and how this critical information is communicated will also be important.

# 4. Possible Future Applications

The starting point of this project was to attempt to understand whether risk management approaches are likely to be interoperable internally within the DND/CF, as well as in conjunction with other government departments. This section explores several possible lines of inquiry to explore this issue further.

## 4.1 Within the Department of National Defence and Canadian Forces (DND/CF)

Future research will need to grapple with the implications of the ongoing DND/CF transformation on the risk management 'landscape'. In spring of 2005, the CF undertook a broad transformation effort working to modernize itself and make it more effective. This transformation led to the creation of four new joint command structures, as well as redefinition of the Strategic Joint Staff. This transformation is also still ongoing. Unfortunately, it is perhaps too early in the DND/CF transformation to access specific writings that would articulate the extent to which the risk management approaches within these relatively new structures will be interoperable. For now, each is bound by the risk management policies prominent in each area. However, understanding exactly how these policies have been (or will be) converted into risk management practice will require more time and/or interviews with personnel representing these different systems.

There are many critical areas within the DND/CF that could be explored with regard to their risk management activities. Given the increased emphasis on joint forces banding together seamlessly, it would be important to understand the degree of congruence in risk management approaches among the Army, Navy and Air Force elements. The ability of these elements to work interoperably is in no way guaranteed simply because they are all part of the CF, and there are distinct cultures impacting relations among them (English, 2001). Using interviews to understand how these risk management processes are seen and managed could be an important contribution to promoting their future interoperability.

With the creation of the Strategic Joint Staff and the four operational joint command forces, the CF has attempted to create a unified and integrated chain of command with the immediate authority to deploy maritime, land, and air forces in support of diverse operations. Although these new command structures are intended to enable a higher level of effectiveness and efficiency in responding to both domestic and international threats, their actual effectiveness is partly dependent on how well these structures will be able to 'mesh' their efforts. This is not to suggest that varying structures must necessarily always be common. In fact, interoperability will require homogeneity in some structures and heterogeneity in others (e.g., different forces have different assets to deploy, but will require similar communication methods). Nonetheless, even heterogeneous structures will need to be able to find common ground to ensure integrated risk management. Another possible area of investigation could be the Joint Staff itself. Tasked with the role of coordinating the operational planning process, the Joint Staff presents a very rich environment in which to study integrated risk management. With the Joint Staff working on many different aspects of the operation (e.g. logistics, personnel, operations, and plans), how these different perspectives on the mission get combined, and indeed, the extent to which the risk management processes that are enacted will be interoperable could make an important contribution to furthering a more coordinated response in the event of a terrorist attack. As such, whatever its focus, additional

research within the DND/CF is necessary to determine the extent to which risk management processes are likely to be effectively aligned among its diverse functions.

## 4.2 The Department of National Defence and Canadian Forces (DND/CF) with Other Government Departments (OGDs)

Another focus of this report was to examine the risk management practices across several departments to determine their level of interoperability in the event of an asymmetric attack. Although all government departments are mandated by the Treasury Board of Canada Secretariat (e.g., 2001) to have risk management procedures in place, the degree to which these are procedures are consistent with other departments is an empirical question. If there are large discrepancies among organizations, responses to an imminent threat such as a terrorist attack could be less effective if focus of the response needs to be on issues of coordination rather than on dealing with the actual threat.

In addition to the DND/CF, future research should target two other departments due to their probable level of involvement responding to a terrorist threat, Public Safety and Emergency Preparedness Canada (PSEPC) and Health Canada. Although limited, the available information related to their response to the Treasury Board of Canada Secretariat's (2001) mandate is considered in the following sections.

### 4.2.1 Public Safety and Emergency Preparedness Canada (PSEPC)

PSEPC is a government department created in 2004 to "ensure coordination across all federal departments responsible for national security and the safety of Canadians" (PSEPC, 2006). PSEPC has about 800 employees, and works in cooperation with six government departments: Canada Border Services Agency, Canada Firearms Centre, Canadian Security Intelligence Service, Correctional Service Canada, Royal Canadian Mounted Police, and the National Parole Board. PSEPC coordinates and support the efforts of these organizations in national emergency management (e.g., operation of critical infrastructure), national security (e.g., advice in monitoring terrorist entities), law enforcement (e.g., intelligence support), corrections (e.g., correctional system policy for community reintegration), and crime prevention (e.g., community-based youth intervention programs). The structure of the PSEPC department is shown in Figure 18.

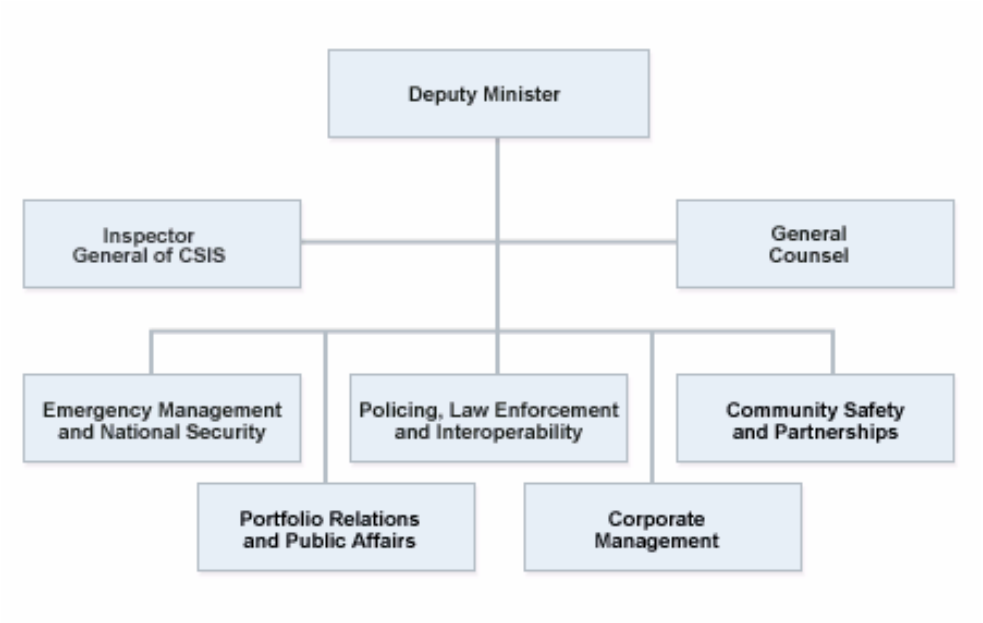


**Figure 18. PSEPC department structure**

Given its mandate, then, PSEPC would likely have a critical role in responding to an asymmetric terrorist attack. Unfortunately, the official risk management policies of PSEPC were not available for this report. However, in other PSEPC documents, the organization stresses that the IRMF will be used as a starting point when developing their national critical-infrastructure-protection strategy. Moreover, in a position paper on critical-infrastructure protection (PSEPC, 2004), PSEPC stated assurance actions for critical-infrastructure protection and noted that the priorities of these actions should be based on risk management principles that employ appropriate common criteria. These criteria include assessing the impact and the consequences of critical infrastructure loss on the operation of the industry. Hopefully, getting access to the risk management policies and approaches used in PSEPC would promote an understanding of its ability to work interoperably with other government departments such as the DND/CF.

### 4.2.2 Health Canada

The ultimate goal of Health Canada is to help Canadians maintain and improve their health (Health Canada, 2007). To carry out this responsibility, the mandate of Health Canada has 4 main components:

- Preserve and modernize Canada's health care system
- Enhance and protect the health of Canadians
- Work in partnership with others, and
- Communicate health promotion and disease prevention

Within this mandate, Health Canada has a number of specific responsibilities. Aside from managing health care costs by communicating health risks and promoting healthy lifestyles, Health Canada provides surveillance, prevention, control and research of disease outbreaks across Canada and around the world. This department also monitors health and safety risks related to the sale and

use of drugs, food, chemicals, pesticides, medical devices, and certain consumer products. Again, given its mandate, Health Canada would be another potential department working with the DND/CF and PSEPC in shaping the Canadian government's response to a potential terrorist attack.

Unfortunately, the risk management policies of Health Canada could not be accessed for this review, but some literature relevant to this was attained. The available literature suggests that the risk management practices of Health Canada are likely to be aligned with national standards as well as the Treasury Board of Canada Secretariat's (2001) framework. In particular, Health Canada appears to have enthusiastically adopted the IRMF and released their plans to implement it in April 2003 (Health Canada, 2004). According to their report, Health Canada elements suitable for integrated risk management include strategic and business planning, performance measurement, the decision-making framework for health risks (a tool for assessing health-related risk), modern comptrollership, program evaluation, values and ethics, internal audit, accountability initiatives, quality assurance units, branch audit groups, technology risk framework, and others.

In particular, Health Canada's departmental executive committee made the following actions in order to promote an integrated approach to risk management:

- Appointed senior officers to lead the risk management initiative and implement integrated risk management in all Branches and Regions.
- Decided to create a network across Branches, Regions and areas of functional expertise that can implement the IRMF and lead the incorporation of risk management into all organizations.
- Assigned the Departmental Executive Sub-Committee on Policy and Analysis to direct and oversee the implementation of an IRMF.
- Identified the Associate Deputy Minister – Corporate Services Branches as the integrated risk management champion to sustain the momentum to a risk-smart environment.
- Assigned the Director, Planning & Special Projects Directorate / Modern Comptrollership Office as the full-time executive for implementing the IRMF, chairs the Integrated Risk Management Network and manages the Office of Integrated Risk Management.

Health Canada planned a phased approach to implementing the IRMF, starting with a *foundation phase* where senior management addressed the basic requirements of the IRMF. This was to be followed by a *transition phase* that would integrate risk management into Health Canada, and finally moving to an ongoing *sustaining phase* where risk management would become an integral part of daily operations and decision-making. To reinforce the transition, Health Canada identified six guiding principles in the transition to the IRMF: commitment, continuity, consistency, communication, culture-conscious, and continuous learning.

Health Canada also identified the need to initiate several key activities corresponding to the four elements of the integrated risk management process: to integrate risk management into existing decision-making processes and in strategic priority setting, to understand risk tolerance, to assess risk management capacity, communicate a corporate risk management direction, share roles and responsibilities within the leadership, and to build on risk management learning. Furthermore, The Department Executive Committee, Office of Integrated Risk Management, and the Treasury Board of Canada Secretariat were identified as needing to have consistent updating and monitoring of Health Canada's progress in adopting the IRMF.

Health Canada (2004) discussed their progress in the development of a corporate risk profile (element 1 of the IRMF) and outlined several goals:

- Ensure that all employees understand planning processes and expected results.
- Development of human resource management strategies and implementation of a Workplace Health and Human Resources Modernization Action Plan.
- Develop management strategies that improve accountability (e.g. values and ethics, internal audit, financial management controls, etc.).
- Pursue legislative and regulatory reforms that keep Health Canada's legislative mandate current with scientific and technological advancements.
- Develop management strategies, such as peer-review programs, that give the department access to quality scientific information as policy issues arise.
- Address long term information technology infrastructure planning.
- Conduct regular external and internal environmental scans to assess relevant factors that could influence HC's operational environment.

Although Health Canada's stated efforts to integrate risk management into their entire organization are encouraging, their reports did not provide more specific information about their risk management strategy. Hopefully, researchers will be able to gain access to these documents in the future.

The extent to which Health Canada and PSEPC might be similar to the six departments reviewed by the Office of the Auditor General of Canada in terms of their maturity on the risk management continuum is unclear, and this will need to be addressed in future research. However, one encouraging estimate derived from the CRS and Deloitte & Touche (2004) review of the DND/CF is that organizations would typically require at least 5 years to achieve a highly mature and integrated risk management process. As it has been several years since their efforts began, all three organizations should have made substantial progress on the risk management maturity continuum.

As such, future research could work to assess the risk management practices across departments and determine if they are in fact aligned. Such assessment might help point to ways in which organizations can promote better coordination of their risk management procedures, and ensure maximal interdepartmental interoperability.

### 4.2.3 Coordination between Government Departments

In addition to the 3 departments which are the focal point of this research (the DND/CF, PSEPC, and Health Canada), many other departments could also be involved, depending on the exact nature of the threat. The readiness of a cross-section of Canadian government departments was examined in a review conducted by the Office of the Auditor General of Canada (2003). This review considered six different government departments (Canadian Heritage, Human Resources Development Canada, Indian and Northern Affairs Canada, the Treasury Board Secretariat, Transport Canada, and Veterans Affairs Canada), and assessed their progress in working toward integrated risk management (as dictated by the Treasury Board of Canada Secretariat). This report noted that despite the commitment to risk management exhibited within these organizations, senior management had not shown enough leadership and commitment to risk management, action plans lacked key elements, risk profiles with clearly defined tolerances were not complete in any of the

six organizations, and some departments had assigned the risk management function to internal audit bodies, which might compromise objective, independent action when necessary. The conclusion of this report was as follows:

> "Generally, we noted a lack of concerted effort across departments to co-ordinate and communicate key information on the initiative. We also found little evidence that departments had made much progress in assessing their capacity for integrated risk management." (Office of the Auditor General of Canada, 2003, p. 8).

This conclusion suggests that Canadian government departments had made relatively little progress more than 2 years after the Treasury Board of Canada Secretariat's (2001) initiative. This same document also indicated some of the elements of the necessary action plans, as shown in Figure 19.

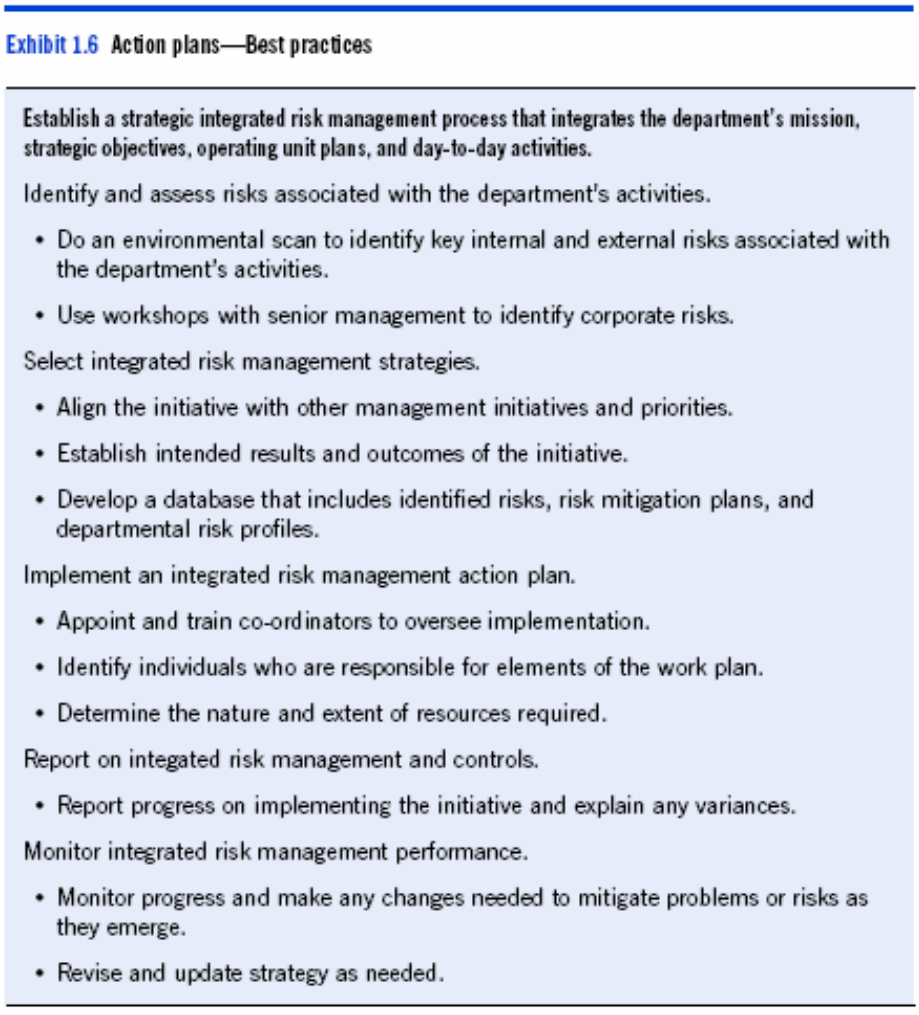

**Exhibit 1.6 Action plans—Best practices**

**Establish a strategic integrated risk management process that integrates the department's mission, strategic objectives, operating unit plans, and day-to-day activities.**

Identify and assess risks associated with the department's activities.

- Do an environmental scan to identify key internal and external risks associated with the department's activities.
- Use workshops with senior management to identify corporate risks.

Select integrated risk management strategies.

- Align the initiative with other management initiatives and priorities.
- Establish intended results and outcomes of the initiative.
- Develop a database that includes identified risks, risk mitigation plans, and departmental risk profiles.

Implement an integrated risk management action plan.

- Appoint and train co-ordinators to oversee implementation.
- Identify individuals who are responsible for elements of the work plan.
- Determine the nature and extent of resources required.

Report on integated risk management and controls.

- Report progress on implementing the initiative and explain any variances.

Monitor integrated risk management performance.

- Monitor progress and make any changes needed to mitigate problems or risks as they emerge.
- Revise and update strategy as needed.

**Figure 19. Office of the Auditor General of Canada - Action plan/best practices (2003, p. 13)**

In assessing the ability of federal government departments to respond to a security risk such as a terrorist attack, two other reports from the Office of the Auditor General of Canada are relevant to this discussion. A report released entitled 'National Security in Canada – The Anti-Terrorist

Initiative' (Office of the Auditor General of Canada, 2004) looked at Canada's post-9/11 security response. The goal of this report was to evaluate the progress that had been made in promoting national security, in part through the creation of new departments such as PSEPC and the Canada Border Services Agency, as well as merging efforts with the DND/CF and the RCMP. Specific areas examined included the coordination of intelligence efforts, the combined ability of the various departments to provide critical information to enforcement personnel, as well as information sharing infrastructures.

That analysis showed that inadequate progress had been made in developing information systems to share information among government departments. The coordination of intelligence information, however, was shown to be particularly problematic. Even for issues of tactical intelligence (i.e., warnings of imminent threat), the Office of the Auditor General of Canada found that

> "…the communication of alerts to a potential threat was sent using the government's top secret messaging system, but was addressed incorrectly. After waiting a month for a response, the sending agency followed up and found that the message had not been received. Fortunately, the alert turned out to be a false alarm." (Office of the Auditor General of Canada, 2004, p. 15)

As the ability to manage risk is predicated on identifying it, this failure is clearly problematic. Another clear problem noted in coordination among government departments attempting to ensure a high level of security was the failure to delineate clear roles and responsibilities, resulting in both unnecessary overlaps and gaps in security. Just as problematic was the lack of an adequate lessons-learned capacity that would help the government learn from its successes and mistakes. As a whole, then, the 2004 report suggested that interoperability in responding to terrorist attacks and other security threats cannot be assumed.

Another report from the Office of the Auditor General of Canada (2005) also addressed the effectiveness of anti-terrorism initiatives started in 2001, targeting air-transportation and marine security as well as emergency preparedness. This review showed that within the air-transportation sector, Transport Canada had yet to implement a formal IRMF throughout the department, even though the processes that were in place were generally consistent with the Treasury Board of Canada Secretariat's (2001) standards.

Within the emergency-preparedness domain, readiness for a chemical, biological, radioactive, or nuclear event was explored with respect to the chain of command, combined national capacity for federal, provincial and municipal coordination, as well as the testing of response plans. This analysis showed that the chain of command was not clearly established, and that there was a lack of common standards and practices that would enable these different levels of government to work seamlessly. Remedying this problem would require having clearer definitions of powers and responsibilities, and these definitions would need to be laid out in the Emergency Preparedness Act to be drafted by PSEPC. In addition, the creation of a new National Emergency Response System was proposed as a method of enabling this coordination. In assessing specific emergency plans in response to a chemical, biological, radioactive, or nuclear event (including National Counter-Terrorism Plan, Food and Agriculture Emergency Response System etc.), the Office of the Auditor General of Canada found that "departmental plans are vague on how they would link together to form a co-ordinated federal response" and there was no way to establish how "…in a complex emergency involving several departments, the plans would work together to achieve a seamless federal response" (Office of the Auditor General of Canada, 2005, pp. 21-22). Moreover, for money that had been allocated to fighting terrorism, there was little evidence of logical allocation of funds based on systematic consideration of risk scenarios.

Although dated, these reports are indicative of the difficulties of coordinating large bureaucracies. Clearly, ensuring a high level of coordination is only possible when institutional roles are clearly defined, adequate infrastructures are in place, and departments have had opportunities to test their ability to be interoperable in typically chaotic environments.

## 4.3 Interoperability Issues to be Explored

Given the information available to date, there is concern about the degree to which government departments, the DND/CF, and other departments would be interoperable in the event of a terrorist attack or other large-scale risk. Certainly, the potential challenges to interoperability within the DND/CF also apply equally in relation to external organizations (see Section 3.2). The Office of the Auditor General of Canada's report (2005) looking at emergency preparedness in Canada provides strong evidence that risk management efforts (as well as other forms of coordination) have the potential to be compromised by problems of interoperability. However, more research will be needed to better understand these issues and to help diagnose the real and potential barriers to achieving effective interoperability.

As noted in the report from the Office of the Auditor General of Canada (2005), whatever level of maturity these complex organizations will have achieved, an apparently overlooked aspect of risk management policies and procedures is the integration of one's own departmental (or organizational) procedures with those of other departments. Although the Treasury Board of Canada Secretariat (2001) focuses on the need to integrate the risk management process into the daily workings of an organization, integration with the approaches of other relevant organizations is not emphasized. As such, available materials only implicitly indicate a need to ensure interoperability amongst all government departments. The repeated need to consider 'all stakeholders' does not adequately address the challenges likely to be faced in actually undertaking a coordinated risk management process. Moreover, there is little obvious recognition in the available documentation about the potential challenges of working with other systems (who may contain stakeholders) that have a very different idea about how a given risk should be managed. As such, current risk management work available to this point lacks any detailed discussion about how all relevant departments can effectively combine their risk management approaches.

In the absence of explicit discussion of how the risk management procedures of different departments could (or should) be merged, one might mistakenly believe that these departments would be able to work relatively independently to manage their piece of 'the puzzle', or that their approaches are consistent enough that they could be easily meshed when it really mattered. Given the lack of coordination inherent in emergency responses to both terrorist attacks (9/11) and natural disasters (such as Hurricane Katrina), it seems critical that the Government of Canada (and, for the purposes of this review, the DND/CF) is not complacent in believing that interoperability is guaranteed even if each government department has an excellent standalone risk management approach. How these approaches will actually be meshed is of critical importance, and an issue that cannot be easily 'ironed out' in an actual emergency situation. Of course, given the limited information that could be accessed for this review, it is possible that policies that speak directly to interagency cooperation may now exist. This will be important to explore in future research.

As such, identification of roles and responsibilities would be critical, within one's own system and potential related systems that would be required to respond to a common threat. An important aspect of interoperability would be transparency in the expectations that each organization has about the role of other organizations in the event of an identified risk. At the very least, for example, given the complex interdependencies amongst the necessary players, it may be helpful to

ensure specification of the many connections between departments given various threat scenarios. Easy access, for example, to information about which departments would need to be contacted in the event of a terrorist attack (and why) might be very helpful. In this sense, even prior to an actual threat, having a clearly defined list of what players need to be involved to initiate a common risk management process would be helpful.

Truly interoperable risk management is likely to be challenged when organizations have differing risk management cultures and are required to approach a common problem. For example, one possible impediment to fully interoperable and integrated risk management procedures is, quite simply, that different organizations may have different goals, and may have very unique priorities when faced with an external threat. For the DND/CF in facing a terrorist threat, for example, the primary interest might be to dispatch the threat, whereas a department such as Health Canada might naturally focus on a very different aspect of the threat (e.g. long-term health damage to the public). These differences in what each organization perceives as the most important risks to mitigate could lead to serious tensions and disagreement that may impact negatively on an effective and coordinated response.

The espoused values and the actual 'values in use' with respect to risk management could also be unique within all the relevant organizations. It is commonly known that formally-endorsed policies are often replaced by informal procedures when crises occur (in fact, this often occurs in day-to-day operations as well). As such, even though an organization may have defined policies regarding the management of risk, the actions taken by members of an organization when actually managing risk may be very different from these formal policies. This can occur for several reasons. It may be that the written policy is overly cumbersome, unclear, or inefficient. Or, employees may simply not be aware of the policy, or may disregard it if they do not agree with it. Regardless of the reason, if informal risk management is being practiced, this could create potentially important inconsistencies in how risk is actually managed. This problem is even more damaging in situations where organizations must merge efforts. High levels of discrepancy between stated values and the actual values in use, of course, would likely impede interoperability because members of different organizations would not necessarily be privy to the unwritten rules of another organization, even if they could access the written policies. For future research, then, it will be necessary to compare written risk management policy to actual risk management practices within each relevant organization. This would require examining both formal and informal procedures as well as gauging the attitudes of personnel within the target systems toward risk management. This analysis would assist in identification of areas of wide discrepancy that would hinder interoperable responses to an external threat, and hopefully enable recommendations that could help to bridge potential gaps. An important part of this research would be to assess the target organizations' ability to engage all personnel in both informal and formal training. Training employees in risk management procedures would be necessary to ensure that everyone is aware of the policy and of their own role in supporting integrated risk management. As such, future research should work to understand the risk management training cycle within each organization.

For future research, then, there are many rich areas of study that could promote a much better understanding of the extent to which government departments such as the DND/CF, Health Canada, and PSEPC are likely to be interoperable in responding to issues like terrorist threats. Enhancing CF interoperability with other departments in the event of a terrorist attack will require studying risk management from both internal (within the CF) and external (e.g. working with other government departments) perspectives. This will require assessing the congruence between formal policies and informal practices, as well as specific attitudes of relevant department personnel. Given the emphasis on risk management being integrated into the everyday workings of an

organization, it will be critical that future research focus on both personnel who are involved with both formal policy (e.g. writing risk management policies), as well engaging personnel who are charged with actually implementing this policy. Only this will provide a more balanced view of the risk management process within a given organization. The next section provides more detail about the critical components of this future research.

# 5. Proposed Method

Fully understanding the potential interoperability of the DND/CF with other government departments (such as PSEPC and Health Canada) will require not only document review but also interviews and/or focus groups with members of relevant departments. Using both questionnaires and structured interviews, this effort would work to determine the level of overlap in attitudes and beliefs about risk management amongst these departments, as well to compare informal and formal risk management procedures within the various departments. This section describes the proposed research approach, development of the study materials, participant considerations, and additional recommendations for future research.

## 5.1 Proposed Research Approach

This section outlines the project requirements, and explores the research tools and methods that could be used for future research. Our assumption at this point is that this research will require identification of participation requirements, policy review, and administration of questionnaires as well as focused interviews. Each of these is discussed in more detail in the following sections.

### 5.1.1 Participant Requirements

Investigations of risk management across departments would require securing a sample as representative as possible from each relevant department. However, achieving this type of sample can be quite difficult and clear criteria would need to be established in order to determine the participants to select for research. To ensure that varying perspectives on risk management could be captured, it would be important that prospective participants come from diverse areas and levels within the organization. This sample would ideally include individuals involved in both developing (e.g., the policy makers) and implementing the risk management process as both play an integral role. This would allow a fuller understanding of the risk management process within each department and would help to ensure that all critical elements of risk management (as outlined by the Treasury Board of Canada Secretariat, 2001) could be assessed.

### 5.1.2 Risk Management Policies and Materials

Having access to all relevant documentation would be necessary for researchers conducting future risk management research; however, there were obstacles in attaining the necessary documents for the purposes of this review. Although the DND/CF doctrine on risk management was available online, this was not the case with PSEPC or Health Canada. As such, it was difficult to assess the degree to which these departments have adopted an integrated approach to risk management. For future research, however, it would be necessary to acquire the formal policy documents.

### 5.1.3 Risk Management Survey

This project included development of a risk management survey that would assist in future research. This survey was designed to assess adherence to risk management 'best practices' indicated by the Treasury Board of Canada Secretariat's (2001) report and other relevant standards (e.g., CSA, 1997), as well as organizational culture and general perceptions of the risk management process within organizations. Exploring these areas would hopefully provide more information

about the extent to which departments involved in responding to identified terrorist threats would be able to coordinate their efforts.

This survey brings together both existing items used in previous risk management research and new items. The study of integrated risk management within the DND/CF performed by the CRS and Deloitte & Touche (2004) presented a diagnostic tool used to assess progress toward integrated risk management within the DND/CF. This tool was adapted slightly for use in this research and addressed several key areas of risk management indicated in the Treasury Board of Canada Secretariat's (2001) Implementation Framework. These areas included:

- Identifying important risks and priorities
- Establishing role and responsibilities for risk management
- Applying integrated risk management approach
- Enabling risk management and learning from experience

In all, twenty-four questions were included from the tool presented by the CRS and Deloitte & Touche (2004).[3] In addition, the CSA guidelines (1997) also discussed other critical elements of risk management that could be explored. These elements were transformed into questionnaire form and included in our diagnostic tool. These nine questions addressed areas such as face-to-face dialogue about the risk management process, stakeholder analysis, documentation, and 3rd-party reviews of risk management procedures

Taken together, these two existing sets of questions provided a good basis for understanding risk management procedures within government departments, but still omitted some of the critical issues noted during the document review for this project that seemed important to address specifically.

Based on our review of the literature, our research team also created a set of questions intended to tap organizational culture. These questions addressed issues such as creativity and flexibility in responding to potential risk management challenges, and also specifically targeted the relationship between the explicit and implicit culture within an organization. Some questions intended to tap informal (vs. formal) risk management approaches ask participants how risk is actually managed in their organization rather than how it 'should' be managed. In all, fifteen questions related to organizational culture were created. Finally, fourteen questions related to general perceptions of (and attitudes toward) the risk management process were also created.

As a whole, then, survey questions can be used to explore risk identification and assessment, roles and responsibilities associated with risk management, application of an integrated risk management approach, organizational culture, and perceptions of risk management. The scale that is proposed for future research consists of sixty-two questions rated on a five-point Likert-type scale, and is shown in Annex E.

A questionnaire containing basic demographic and experiential information was also created. Specifically, the background questionnaire includes participants' experience in the DND/CF, their experience working in the organization, and level of risk management training both within and external to their respective departments.

[3] It is important to note that, if accessible, data from the earlier CRS review (CRS & Deloitte & Touche, 2004) could presumably be used as a 'baseline' indicator of progress made by the DND/CF since the last review.

Using the diagnostic tool developed for this research, participants from each organization would answer questions regarding their risk management procedures. Responses to the questionnaire would provide information on the organization's approach to risk management, including how they define risk, identify risks, and establish roles and responsibilities. It would also indicate the extent to which the organization takes an integrated approach to risk management, and how their organization culture influences their risk management practices. Once responses about informal risk management procedures and risk management culture are acquired, these can later be compared with the organizations' formal documentation.

### 5.1.4 Interviews

Interviews would help to acquire an in-depth view of the organizations' risk management practices. These interviews could be conducted in either a structured or semi-structured format, with costs and benefits to each approach. Adopting a more structured protocol would provide more consistency across participants, but may limit the ability to follow up on the flow of conversation. Important points made by the participant may be overlooked if inconsistent with the protocol, or followed up in a different order than might be ideal for the participant. However, a less-structured format might facilitate more natural conversation in keeping with the participants' own pace but offers less consistency. Whatever approach is decided on for future research, it will be necessary to ensure that there is the best possible balance of consistency and participant engagement in the research.

For future research, it should be noted that there is also the option to conduct focus groups in lieu of interviews. With a focus-group approach, participants from the same organization (or even different departments) could discuss their risk management policies and procedures in a common forum. This approach may be beneficial from a time and cost perspective. In addition, group discussions may generate more information as an open forum may help individuals bring forth critical information that they would otherwise not have thought to discuss. However, some participants may be hesitant to openly discuss their views on how risk management is carried out in their organization. This may be especially true if there are power inequities among participants. That is, participants may be less inclined to discuss their perspective if their superiors were in the same room. These cost and benefits need to be considered in deciding which approach would best suit this research.

Some preliminary questions that could be used as a basis for future research are presented in Annex E. These questions relate to issues of risk identification and analysis, as well as specifically addressing organizational culture in more flexible way than the survey would allow. Developing a more detailed set of questions would be necessary for future research. This, however, would require specific knowledge of the exact pool of participants to be sampled, in order to tailor the interview to their specific domain.

## 5.2 Overview and Future Challenges

Having collected information for each organization, analyses would be conducted comparing responses across the different organizations. This would assist identification of whether the various departments have similar risk management policies and practices, as well as the extent to which they are likely to be interoperable when faced with a threat such as a terrorist attack. Hopefully, the materials created for this study will help identification of which elements are in agreement (or disagreement), as well as allow comparison to existing standards. For instance, PSEPC and Health

Canada may have very similar approaches to risk management; however, in the event of an identified threat, their risk management culture may make their actual responses very divergent.

For future research, there are several potential challenges that would need to be overcome. These are both pragmatic and conceptual. At the pragmatic level (as noted earlier), access to both participants and relevant materials (e.g. actual risk management policies of government departments) will be critical. Our experience in this study suggests that conducting such research will require effective and efficient liasons that can put researchers in contact with organisational representatives that are willing to provide support for the research in terms of motivating others in the organisation to speak candidly about the relevant issues. Without a known point of contact (or introduction from within the organization), individuals from such government organizations may be very hesitant to discuss topics such as risk management.

Several conceptual challenges are likely to present themselves in the study of interoperable risk management both within the DND/CF and between it and other governmental departments. The challenge is in defining what exactly is meant by 'interoperability'. CF's Joint Operating Concept 2012 (DND, 2003) defines interoperability from three perspectives: information interoperability (the way information is shared, including technological and procedural aspects); cognitive interoperability (the way we perceive and think, as reflected in doctrine and decision processes); and behavioural interoperability (the implementation of the selected COA). In the context of risk management, however, it would be important to identify exactly what interoperability might mean. For example, would ensuring interoperability amongst departments mean that their risk management procedures are completely aligned (both in terms of formal policy and organizational culture) or simply that their procedures are compatible? Exactly how interoperability is conceptualized is likely to be critical for both practice and research, and this will be no less critical for the proposed program of research.

Another potential challenge to the proposed research is that risk management sometimes appears to be seen more as a set of discrete procedures than as a core culture change and transformation. This may put more emphasis than optimal on the 'nuts and bolts' of risk management, and not enough on how an organization can actually work to induce this broader form of change. Even reading all the risk management standards provides relatively little information about how to facilitate the deep cultural changes that would need to occur in working toward integrated risk management. Moreover, policies and guidelines depict risk management as a set of discrete steps in a very orderly process. A potential problem with this perspective, however, is that responding to an actual risk management event may be very different from this orderly sequence of 'if X, then Y'. One important issue to explore in the interviews is how to facilitate the highest possible level of situation awareness of the risk management process itself. How one determines the next logical step in the risk management process obviously depends on where one is in that process. As such, attention needs to be paid not only to what the proper steps in the sequence might be, but also to what evidence would be most relevant to tracking the risk management process as it is unfolding. Only then will it be possible to know how to mesh one's own efforts with those of other parties.

As noted earlier, an important focus of this research is on understanding the level of congruence between explicit risk management policies and how risk management procedures are actually enacted. Maintaining this broader focus, and being able to find the implicit messages within the explicit information elicited within this research will be of critical importance.

Another potential challenge for future research in this area may stem from the difficulties of articulating general procedures without reference to specific cases. .Of course, at a general level, it would be possible to have participants provide a 'broad strokes' account of what their organization

would do in the event of a risk such as a terrorist attack, but it seems unlikely that this account would provide enough detail to fully expose potential differences in organizational approaches that might undermine interagency cooperation.

One alternative possible in future research would be to have participants work through hypothetical risk scenarios and determine their individual/organizational responses to these scenarios. For example, creating scenarios in which an asymmetric terrorist attack had occurred would be another way to investigate interoperability.[4] Some examples of issues that could be explored include:

- Given the scenario described, what communications would be initiated by your organization and why? Whose responsibility is it to initiate these communications? What other departments would you expect would initiate contact with your organization and why?
- At what point in the hypothetical risk scenario do you believe that your organization would identify the risk? What characteristics are important in making this determination?
- What specific aspects of the risk related to the event (e.g., terrorist attack) do you see as your organization's responsibility?
- Of the remaining risks (identified in the scenario or elicited), please assign responsibility to the other organizations involved

The level of fidelity of this simulation could, of course, vary widely. At the high end of the scale, creating a risk management scenario (such as a terrorist threat) that linked diverse organizations while offering real-time updates and an interactive interface would help participants be immersed in the scenario and simulate some of the pressures likely to be faced. Providing a richer set of stimuli may yield a more complex account of the potential challenges to interoperability.

Observations of these scenarios could then be compared with written policy to determine whether participants followed their organization's procedures in working through the scenario, or whether they engaged in informal risk management actions. Overall, the extent to which the approaches of the organizations involved would be interoperable would provide important information about Canada's readiness in the event of a terrorist attack, and about the work that remains to be done as departments move toward a more mature and integrated risk management approach. Clearly, the time to explore ways in which to 'mesh' risk management efforts is not in the midst of a crisis.

These ideas, of course, represent only the tip of the iceberg in terms of what future research could explore and contribute. The documents reviewed in this research provide a good grounding for future work exploring risk management interoperability in relation to the DND/CF. Both implicitly and explicitly, they indicate willingness to work to further integrated risk management within the DND/CF (and other government departments), as well as the need for more work to be done. The analysis and proposed research undertaken in this report could provide a sound basis for future research aimed at better understanding and promoting higher levels of interoperability in managing risk.

[4]Of course, it is possible that some scenario-based simulations conducted by the CF may have already explored risk management processes to some extent.


This page intentionally left blank.

# References


The Association of Insurance and Risk Managers (AIRMIC), Association of Local Authority Risk Mangers: The National Forum for Risk Management in the Public Sector (ALARM), & The Institute of Risk Management (IRM) (2002). *A risk management standard.* Retrieved February 24th, 2006, from IRM Web site http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Canadian Standards Association (CSA). (1997). Risk management: Guideline for decision-makers. A national standard of Canada.

Chief Review Services (CRS) & Deloitte & Touche. (2004). Baseline study: Integrated risk management within the DND/CF.

Canadian Security Intelligence Service (CSIS). (2002). Backgrounder no. 8: Counter-terrorism. Available online on the CSIS Web site: http://www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder08.asp

CTV.ca News Staff. (July 8th, 2005). Canada increases vigilance after London Attacks. Retrieved March 20th, 2006 from CTV.ca Web site: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20050708/canada_security_050707?s_name=&no_ads=

CTV.ca News Staff. (July 11th, 2005). Canada is potential terrorist target: Hillier. Retrieved March 20th, 2006, CTV.ca Web site: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1121016031941_16/?hub=TopStories

Department of National Defence (2002). Risk management for CF operations.

Department of National Defence (DND). (n. d.) Goals of the Department of National Defence (DND) and the Canadian Forces (CF). Retrieved March 16th, 2007 from Department of National Defence Web site: http://www.forces.gc.ca/site/faq/Answers_e.asp#three1

Department of National Defence (DND). (2005a). Integrated risk management guidelines.

Department of National Defence (DND). (2003). CF Joint Operating Concept 2012.

Department of National Defence (DND). (2005b). Integrated risk management policy.

English, A. (2001). Understanding military culture. Report produced for Defence Research and Development Canada.

Health Canada (2004). Overview: Health Canada's progress towards an Integrated Risk Management Framework.

Health Canada (2007). Webpage available at http://www.hc-sc.gc.ca/ahc-asc/activit/index_e.html.

Johnson, K., Locy, T., & Kiely, K. (July 22nd, 2003). *9/11 panel blasts CIA, FBI's lapses in coming report.* Retrieved March 21st, 2006, from USA TODAY Web site: http://www.usatoday.com/news/washington/2003-07-21-intel-usat_x.htm

Office of the Auditor General of Canada. (2003). Chapter 1 – Integrated Risk Management.

Office of the Auditor General of Canada. (2004). Chapter 3. National Security in Canada - The 2001 Anti-Terrorism Initiative.

Office of the Auditor General of Canada. (2005). Chapter 2. National Security in Canada - The 2001 Anti-Terrorism Initiative: Air Transportation Security, Marine Security and Emergency Preparedness.

Public Safety and Emergency Preparedness Canada (PSEPC). (2004). Government of Canada position paper on a national strategy for critical infrastructure protection.

Public Safety and Emergency Preparedness Canada (PSEPC). (2006). *About Us.* Retrieved March 16th, 2006, from PSEPC Web site: http://www.psepc-sppcc.gc.ca/abt/index-en.asp

Standards Australia and Standards New Zealand. (2004). *Risk Management*. Sydney: Standards Australia.

Treasury Board of Canada Secretariat. (2001). Integrated Risk Management Framework (Cat. No. BT22-78/2001). Retrieved January 31st, 2006 from Treasury Board of Canada Secretariat Web site: http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

Treasury Board of Canada Secretariat. (2003). Integrated Risk Management Implementation Guide. Retrieved January 31st, 2006 from Treasury Board of Canada Secretariat Web site: http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

# Acronyms

| | |
|---|---|
| AIRMIC | Association of Insurance and Risk Managers |
| ALARM | Association of Local Authority Risk Managers |
| COA | course of action |
| CRS | Chief Review Services |
| CSA | Canadian Standards Association |
| DND/CF | Department of National Defence and Canadian Forces |
| IRM | Institute of Risk Management |
| IRMF | Integrated Risk Management Framework |
| NGOs | Non-Governmental Organizations |
| OGDs | Other Government Departments |
| PSEPC | Public Security and Emergency Preparedness Canada |
| RCMP | Royal Canadian Mounted Police |
| VCDS | Vice-Chief of Defence Staff |


This page intentionally left blank.

# Annex A.

Risk-Analysis Methods (AIRMIC, ALARM, & IRM, 2002, p. 14)

Upside risks

- Market Survey
- Prospecting
- Test marketing
- Research and development
- Business impact analysis

Both

- Dependency modelling
- SWOT (Strength, Weaknesses, Opportunities, Threats) Analysis (Mindtools, n. d.)
- Event tree analysis (The Institute of Electric Engineers, 2004)
- Business continuity planning
- BPEST (Business, Political, Economic, Social, Technological) analysis
- Real Option Modelling
- Decision taking under conditions of risk and uncertainty
- Statistical inference
- Measures of central tendency and dispersion
- PESTLE (Political Economic Social Technical Legal Environment) (Thames Valley University, n. d.)

Downside risk

- Threat analysis
- Fault tree analysis (The Institute of Electrical Engineers, 2004)
- FMEA (Failure Mode & Effect Analysis)

This page intentionally left blank.

# Annex B.

Examples of Possible Risk Estimation Methods (AIRMIC, ALARM, & IRM, 2002, p.7)

| | |
|---|---|
| High | Financial impact on the organisation is likely to exceed £x<br>Significant impact on the organisation's strategy or operational activities<br>Significant stakeholder concern |
| Medium | Financial impact on the organisation likely to be between £x and £y<br>Moderate impact on the organisation's strategy or operational activities<br>Moderate stakeholder concern |
| Low | Financial impact on the organisation likely to be less that £y<br>Low impact on the organisation's strategy or operational activities<br>Low stakeholder concern |

| Estimation | Description | Indicators |
|---|---|---|
| High (Probable) | Likely to occur each year or more than 25% chance of occurrence. | Potential of it occurring several times within the time period (for example - ten years).<br>Has occurred recently. |
| Medium (Possible) | Likely to occur in a ten year time period or less than 25% chance of occurrence. | Could occur more than once within the time period (for example - ten years).<br>Could be difficult to control due to some external influences.<br>Is there a history of occurrence? |
| Low (Remote) | Not likely to occur in a ten year period or less than 2% chance of occurrence. | Has not occurred.<br>Unlikely to occur. |

| Estimation | Description | Indicators |
|---|---|---|
| High (Probable) | Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence. | Clear opportunity which can be relied on with reasonable certainty, to be achieved in the short term based on current management processes. |
| Medium (Possible) | Reasonable prospects of favourable results in one year of 25% to 75% chance of occurrence. | Opportunities which may be achievable but which require careful management. Opportunities which may arise over and above the plan. |
| Low (Remote) | Some chance of favourable outcome in the medium term or less than 25% chance of occurrence. | Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood of success is low on the basis of management resources currently being applied. |

# Annex C

(1) J-1 (Personnel)

(a) Estimate time delay risks on personnel deployment flow;

(b) With J2 input, determine casualty risks for each COA;

(c) Estimate casualty and replacement flow risks on future operations;

(d) Ensure controls for personnel-related activities are conducted to diminish operations security vulnerabilities and support military deception initiatives; and

(e) Estimate risks of employed local civilian labour in coordination with the J-4 (logistics), J-2 (intelligence) and legal officer.

(2) J-2 (Intelligence)

(a) Monitor and report threats that counter the effectiveness of friendly combat identification/counter-fratricide measures;

(b) Develop current regional threat assessments;

(c) Develop terrain and climate assessment; and

(d) Determine risk of loss of low-density intelligence collection assets.

(3) J-3 (Operations)

(a) Develop risk assessment for the commander's estimate;

(b) Perform as staff proponent for combat identification/counter-fratricide measures;

(c) Develop policy, procedures and assign responsibility for combat identification/counter-fratricide measures;

(d) Report and investigate reports of fratricides;

(e) Develop risk assessment of military and political aspects of draft ROE and supplemental ROE; and

(f) Determine criticality and vulnerability of bases in the Joint Rear Area to prioritize controls and levels of response.

(4) J-4 (Logistics)

(a) Assess the risk of critical supply levels not meeting required number of days of supply;

(b) Determine petroleum, oils, and lubricants storage site vulnerabilities and controls; and

(c) Determine munitions storage site vulnerabilities and safety requirements

(5) J-5 (Plans)

(a) Integrate functional directorate risk management controls and combat identification/counter-fratricide measures into deliberate planning products; and

(b) Identify friendly manoeuvre and firepower vulnerabilities during mission analysis, war gaming and plan controls to mitigate risk.

(6) J-6 (Communications): Responsible for assessing risk to geospatial information and services systems and developing controls to counter threats.

(7) J-5 (PA). The lack, or inadequate application, of the PAff function in CF Ops could lead to adverse perceptions, on the part of national or international audiences thereby affect the Commander's ability to attain a planned end-state. The J-5 (PA) staff will assess, develop and implement controls for risk associated with the following:

(a) the provision and dissemination of information (OPSEC vs public's right to know);

(b) inaccurate messaging of public policy;

(c) inadequate support of personnel and equipment;

(d) inadequate PAff training (all personnel including PAff staffs); and

(e) inaccurate advice and guidance to the Commander, his staff and members of the mission.

(8) Special staff offices: Risk management should be addressed by various special staff offices:

(a) J4 HSS (health and non-battle injury, return to duty policy, preventative medicine).

(b) J5 Legal (Canadian and international law, law of armed conflict, and host nation (HN) law).

(c) J8 Fin. Ensure commanders are aware of the financial implications of decisions by providing timely and accurate analysis and advice on incremental costs, funding sources and requisite approval authorities associated with each COA.

(d) Safety officer

# Annex D

**Participant #** _____ **Date and Time** _____

**Tape #** _____ **Location** _____

**Please provide the requested background information in the spaces provided.**

| **Demographics:** | | | | | |
|---|---|---|---|---|---|
| ***What year were you born in?*** _____ | | | | | |
| **First Language** English ○ French ○ Other (specify) _____ | | | | | |
| **What country were you born in?** Canada ○ Other (specify) _____ | | | | | |
| **Experience:** | | | | | |
| **Agency** **CF** ○ **DND** ○ **PSEPC** ○ **RCMP** ○ **HEALTH CANADA** ○ | | | | | |
| **If CF, what element?** **Army** ○ **Navy** ○ **Air Force** ○ | | | | | |
| **Current Position:** | | | | | |
| **How long have you worked at your current organization?** | | | | | |
| Up to 10 years | 10 to 15 years | 15 to 20 years | 20 to 25 | 25 to 30 | More than 30 |
| ○ | ○ | ○ | ○ | ○ | ○ |
| **Rate the amount of <u>training in risk management</u> that you have received within your organization.** | | | | | |
| **None** | **Some** | **Moderate** | **Extensive** | | |
| ○ | ○ | ○ | ○ | | |
| **Rate the quality of <u>training in risk management</u> that you have received within your organization.** | | | | | |
| **Very Poor** | **Poor** | **Good** | **Very Good** | | |
| ○ | ○ | ○ | ○ | | |
| **Rate the amount of <u>training in risk management</u> that you have received external to your organization.** | | | | | |
| **None** | **Some** | **Moderate** | **Extensive** | | |
| ○ | ○ | ○ | ○ | | |
| **Rate the quality of <u>training in risk management</u> that you have received external to your organization.** | | | | | |
| **Very Poor** | **Poor** | **Good** | **Very Good** | | |
| ○ | ○ | ○ | ○ | | |

This page intentionally left blank.

# Annex E

**Interoperable Risk Management in a Joint Interagency Environment - Draft Survey**

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>to help determine the extent to which<br>integrated risk management is being practiced<br><br>Never 1 ☐ 2 ☐ 3 ☐ Sometimes 4 ☐ Always 5 ☐ \| Don't know / Doesn't Apply ☐ | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 1 – IDENTIFYING IMPORTANT RISKS AND PRIORITIES** | | |
| 1. A common definition of risk is used across the organization (e.g., when people discuss risk, it means the same thing throughout the organization). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 2. Risk tolerances are understood (e.g., there is an understanding of the degree of risk that is acceptable within your organization). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 3. The environment is scanned and potential risks are identified on a regular basis (e.g., sources of risk, opportunities and threats are regularly reviewed). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 4. Important risks are formally assessed, using established criteria, on a regular basis (e.g., the assessment of risks is done in terms of impact and likelihood). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 5. Important risks are monitored on an ongoing basis (e.g., there are regular forums for senior managers where risks are reviewed. Actions to mitigate these risks are also discussed). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 6. Risk management priorities are in line with organizational objectives (e.g., risks are prioritized for action and these priorities line up with the priorities of the organization). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>to help determine the extent to which<br>integrated risk management is being practiced<br><br>Never 1 2 3 4 5 Always \| Don't know / Doesn't Apply | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 2 – ESTABLISHING ROLES AND RESPONSIBILITIES FOR RISK MANAGEMENT** | | |
| 7. Risk management strategies are understood (e.g., there is clear direction as to how risks are to be managed within your organization. Objectives and policies are in place). | 1 2 3 4 5 \| | |
| 8. A risk management Office of Principal Interest provides support (e.g. there is a designated champion for risk management and this champion provides direction and disseminates information and best practices regarding risk management). | 1 2 3 4 5 \| | |
| 9. Stakeholders are informed of important risks (e.g., those that contribute or could be impacted are kept informed of significant risks). | 1 2 3 4 5 \| | |
| 10. Roles and responsibilities for managing risks are understood (e.g., it is clear that everyone has a role in managing risk within your organization and they know they need to do so. There are designated risk owners and risk managers). | 1 2 3 4 5 \| | |
| 11. Individuals with accountability for managing risks have the required authority (e.g., the risk owners and managers have the necessary authority to act. Risks are not assigned to individuals who do not have authority to deal with them). | 1 2 3 4 5 \| | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>to help determine the extent to which<br>integrated risk management is being practiced<br><br>Never 1 2 3 4 5 Always \| Don't know / Doesn't Apply | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 3 – APPLYING AN INTEGRATED RISK MANAGEMENT APPROACH** | | |
| 12. Overall, there is a defined process for risk management (e.g., the process to be followed within your organization to identify, act upon and monitor risks is clear to all individuals). | 1 2 3 4 5 \| | |
| 13. Practices for managing risks are consistently applied (e.g., the approach to managing risks is aligned throughout your organization). | 1 2 3 4 5 \| | |
| 14. Tools, methods and techniques are used for managing risk (e.g., there is a common model, frameworks or template used to identify, assess, record and monitor risks). | 1 2 3 4 5 \| | |
| 15. Risks are addressed as part of the planning process (e.g., risks are identified and monitored, and mitigating strategies and action plans are developed as part of the planning process). | 1 2 3 4 5 \| | |
| 16. Important decisions involve an analysis of underlying risks (e.g., key decisions take into account risk considerations). | 1 2 3 4 5 \| | |
| 17. There is a linkage between performance measures and risk (e.g., performance measures have been established that relate to risks within the organization). | 1 2 3 4 5 \| | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>to help determine the extent to which<br>integrated risk management is being practiced<br><br>Never 1 ☐ 2 ☐ 3 ☐ Sometimes 4 ☐ Always 5 ☐ \| Don't know / Doesn't Apply ☐ | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| 18. Practices for managing risks are monitored for effectiveness (e.g., risk management activities are regularly reviewed using metrics to ensure they contribute to effectively managing risk, and changes are implemented). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 19. Risk management information is reported (e.g., there are reports prepared which highlight risks and risk mitigation activities at every level). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 20. Risk information is shared within your organization, with other organizations or on a department-wide basis (e.g., risk information is discussed with other groups proactively, with the management of risks adjusted accordingly). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 21. Technology is used to store risk information and to facilitate reporting (e.g., a software system is used to log risk information and facilitate the aggregation and reporting of information to senior management). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>to help determine the extent to which<br>integrated risk management is being practiced<br><br>Never 1 2 3 4 5 Always \| Don't know / Doesn't Apply | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 4 – ENABLING RISK MANAGEMENT AND LEARNING FROM EXPERIENCE** | | |
| 22. Organizational culture supports effective risk management (e.g., there is open communication about risks, people are encouraged to identify and discuss risks and propose innovative ways to deal with risk). | 1 2 3 4 5 \| | |
| 23. Training on risk management concepts and fundamental theory is provided to improve risk management competencies (e.g., training has been developed and implemented to ensure L1 individuals involved in risk management have the right skills and competencies. Training is available and ongoing). | 1 2 3 4 5 \| | |
| 24. Within the organization, there is recognition for managing risks. | 1 2 3 4 5 \| | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 5 – CSA Standard** | | |
| 25. Face-to-face, two-way dialogue is practiced throughout the risk management process. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 26. Steps are taken on an ongoing basis to identify potential stakeholders. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 27. Extensive documentation (record-keeping) is applied throughout the risk management process (e.g., risk information library). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 28. The risk management team consists of experts from multiple disciplines. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 29. The risk management process is defined by explicit stages. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 30. An objective third-party reviews the risk management process. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 31. Risk communication with stakeholders happens throughout the risk management process. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| 32. Implicit, soft benefits/costs are recognized in addition to explicit or hard benefits/costs (e.g., reduction in quality of life vs. financial loss). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 33. Public perceptions of the risk are taken into account during the risk management process. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br><br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 6 – Organizational Culture** | | |
| 34. People are open to communicate potential risks to superiors. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 35. Informal discussions of risk exist. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 36. There is an orientation within the organization to strive to identify new areas for development. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 37. There is unity in how risk management challenges are approached within the organization. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 38. The organization focuses on rewarding those who identify problems in addition to those who achieve results. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 39. Those who discover and report risk management flaws are perceived as productive employees. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| 40. A common language for risk management is a problem within the organization. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 41. All organization personnel take initiative in risk management. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 42. Information important to risk management is treated as confidential for no apparent reason. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |
| 43. There is an emphasis on teamwork to achieve risk management objectives. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| 44. The experimentation and exploration to identify new opportunities in relation to risk management is tolerated. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 45. Accountability within the risk management process is correctly aligned with the assigned level of authority. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 46. There are incentives for personnel to engage in the risk management process. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 47. There are interactive training tools for risk management available in your organization. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 48. Risk management in the organization is based on a flexible process that tolerates regular changes and review. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |

| **STATEMENTS**<br>to help gather relevant information<br>in relation to integrated risk management<br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| **PART 7 - Perceptions of Risk Management** | | |
| 49. Taking into account costs and benefits, risk management is worth doing. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 50. Risk management is important to the goals and objectives of the organization. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 51. There are organizational-based problems in perceiving relevant risks. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 52. There are individual-based problems in perceiving relevant risks. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 53. The frequency and consequence of risks are effectively assessed. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 54. The department's risk management strategy is not effective. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 55. The department's risk management strategy is prepared to deal with asymmetric threats, such as terrorism. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |
| 56. The responsibilities of the risk management team are clearly defined. | 1 2 3 4 5 ☐ ☐ ☐ ☐ ☐ ☐ | |

| **STATEMENTS**<br>to help gather relevant information in relation to integrated risk management<br>**Please respond in relation to your organization** | **SCALE**<br>To help assess the extent to which you agree with these statements<br>Strongly Disagree / Somewhat / Strongly Agree / Don't know / Doesn't Apply<br>1 2 3 4 5 | **COMMENTS**<br>to provide examples in relation to the statements and scale |
|---|---|---|
| 57. An interdepartmental standard for safety and security risk assessment is necessary for the well-being of the organization. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 58. An interdepartmental standard for safety and security risk assessments has already been met by current interdepartmental policies and practices (e.g., there is a risk communication function). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 59. Public perceptions of risk, which are often different from expert or scientific assessments, are valid (e.g., nuclear power plant safety). | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 60. An interdepartmental standard for safety and security risk assessments has already been met by current interdepartmental policies and practices. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 61. Are there are sufficient mechanisms to create trust in risk management policies between departments within the organization, amongst organizations and with the public. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |
| 62. The department's explicit risk management policies are congruent with how things are actually done. | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ \| ☐ | |

# Interview Questions

| |
|---|
| Risk Identification and Analysis |
| 1. What criteria are used to identify acceptable levels of risk? Who determines this? |
| 2. What kinds of events are likely to initiate a formal risk management process? |
| 3. What kinds of tools and techniques are being used to manage risk in your organization? |
| 4. What steps are taken to identify, analyze, and develop a profile of potential stakeholders? What defines a stakeholder? |
| 5. What strategies or analytical techniques are used to identify risks? (e.g. Fault-tree analysis, event-tree analysis, mathematical, and econometric model) |
| 6. What kind of documentation does your department require during and after risk management procedures are enacted? |
| Organizational Culture |
| 1. Would you say that your organization's approach to risk management is reactive or proactive? |
| 2. To what extent is the formal risk management policy consistent with what you and your organization's members actually do? |
| 3. How consistent is the risk management culture in your organization with those of your peers in other organizations? |
| Perceptions of Risk Management |
| 1. Who should be included as stakeholders in the risk management process? |
| 2. How do stakeholders' needs differ across departments? |
| 3. In military and anti-terrorism contexts, absolute transparency with stakeholders is not possible - where does one draw the line in risk communication? |
| 4. Have there been situations in your department or department where acknowledging risks led to negative outcomes? What happened, and why? |
| 5. What percentage of your organization's resources should be spent on risk management? |
| 6. To what extent do the controls necessary for effective risk management facilitate or impede organization performance? |

**DOCUMENT CONTROL DATA**
(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document, Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's document, or tasking agency, are entered in section 8.)

Publishing: DRDC Toronto

Performing: Humansystems Incorporated 111 Farquhar St., 2nd floor, Guelph, ON N1H 3N4o

Monitoring:

Contracting: DRDC Toronto

2. SECURITY CLASSIFICATION
(Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification is indicated by the appropriate abbreviation (S, C, R, or U) in parenthesis at the end of the title)

Interoperable Risk Management in a Joint Interagency Multinational Environment (U)
La gestion des risques interopérables dans un environnement interarmées multinational et multiorganisationnel (U)

4. AUTHORS (First name, middle initial and last name. If military, show rank, e.g. Maj. John E. Doe.)

Barbara D. Adams; Sonya Waldherr ; Kenneth Lee

5. DATE OF PUBLICATION
(Month and year of publication of document.)

September 2007

6a NO. OF PAGES
(Total containing information, including Annexes, Appendices, etc.)

81

6b. NO. OF REFS
(Total cited in document.)

18

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of document, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The names of the department project office or laboratory sponsoring the research and development − include address.)

Sponsoring:

Tasking:

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant under which the document was written. Please specify whether project or grant.)

15AT33−01

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7711−047911/001/TOR

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document)

DRDC Toronto CR 2007−068

10b. OTHER DOCUMENT NO(s). (Any other numbers under which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on the dissemination of the document, other than those imposed by security classification.)

Unlimited distribution

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11), However, when further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited announcement

**DOCUMENT CONTROL DATA**
(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

(U) This report addresses risk management in the Department of National Defence and Canadian Forces, and explores the extent to which DND/CF is likely to be interoperable internally (e.g. in joint operations), as well as in relation to other organizations in the event of a major threat such as a terrorist attack.

This report first explores existing national standards for conducting risk management, as well as the Treasury Board's integrated risk management framework (2001) that mandates all government agencies in Canada to have a risk management plan. The available risk management approach of DND/CF (available in existing doctrine) is then considered in relation to the approach mandated by the Treasury Board. A review by Chief Review Services (2004) also provided a detailed assessment of the progress that DND/CF had made in implementing an integrated risk management plan.

Review of these documents suggests some cause for concern with respect to future interoperability. Specifically, one potential problem (also noted in the CRS review) are the 2 distinct cultures within DND/CF with respect to risk management, and these cultural differences were no less prominent in 2005 documents provided by DND/CF in response to the CRS review. In general, the need for a common definition of risk management was also evident, as was a potential disconnect between the explicit risk management policies and the implicit approaches likely to be taken in an actual risk or threat situation.

Other articles were reviewed to explore the potential interoperability of DND/CF in relation to other government departments such as Public Security and Emergency Preparedness (PSEPC) and Health Canada. Auditor General reports, for example, showed that the progress of other government departments in working toward integrated risk management was slower than optimal (2003), and that even the specific departments charged with emergency preparedness had not established a clear chain of command, showed a lack of common standards and practices, and had failed to be interoperable even in their everyday workings (2005). These problems are likely to deter significantly from risk management efforts.

The final chapter of this report describes a research approach that would explore risk management within DND/CF as well as in relation to other government agencies likely to be implicated in responding to terrorist threats. Lastly, this report details the creation of research questionnaires that could be used to further explore these issues, and the questions that could be used in face−to−face interviews. Other possible research approaches are also discussed, including the development of risk management scenarios. Hopefully, the work undertaken in this project will provide a sound base for future research working to understand and promote higher levels of interoperability in managing risk.

(U) Ce rapport porte sur la gestion des risques au sein du ministère de la Défense nationale et des Forces canadiennes, et il montre dans quelle mesure le MDN/les FC sont susceptibles d'être interopérables à l'interne (p. ex., au cours d'opérations interarmées) et lorsqu'ils sont en relation avec d'autres organisations gouvernementales en cas de menace sérieuse telle qu'un attentat terroriste.

Ce rapport traite d'abord des normes nationales existantes en matière de gestion des risques, de même que du Cadre de gestion intégrée des risques du Conseil du Trésor (2001), qui oblige tous les organismes gouvernementaux canadiens à avoir un plan de gestion des risques. L'approche de gestion des risques actuelle du MDN/des FC (qui se trouve dans la doctrine actuelle) est ensuite examinée par rapport à l'approche rendue obligatoire par le Conseil du Trésor. Un examen effectué par le Chef – Service d'examen

(2004) a également fourni une évaluation approfondie des progrès faits par le MND/les FC en ce qui a trait à la mise en œuvre d'un plan de gestion intégrée des risques.
L'examen de ces documents suscite certaines préoccupations en ce qui concerne l'interopérabilité future. Plus particulièrement, les deux cultures distinctes présentes au sein du MDN/des FC en matière de gestion des risques constituent un problème potentiel (également indiqué dans l'examen du CS Ex), et ces différences culturelles n'étaient pas moins évidentes dans les documents qu'ont fournis le MDN/les FC en 2005 en réaction à l'examen du CS Ex. En général, le besoin d'une définition commune de la gestion des risques était également évident, comme l'était la possibilité d'une rupture entre les politiques de gestion des risques explicites et les approches implicites susceptibles d'être utilisées dans une situation réelle comportant un risque ou une menace.
D'autres articles ont été examinés en vue d'étudier l'interopérabilité potentielle du MDN/des FC lorsqu'ils sont en relation avec d'autres ministères comme Sécurité publique et Protection civile Canada (SPPCC) et Santé Canada. Par exemple, des rapports du vérificateur général ont montré que les progrès accomplis par d'autres ministères quant au travail relatif à la gestion intégrée des risques étaient plutôt lents (2003) et que même les ministères particuliers chargés de la protection civile n'avaient pas établi une chaîne de commandement claire, n'avaient pas de normes et de pratiques communes et qu'ils n'étaient même pas interopérables dans leur fonctionnement de tous les jours (2005). Ces problèmes sont susceptibles d'avoir un effet dissuasif important relativement aux efforts en matière de gestion des risques.
Le dernier chapitre de ce rapport décrit une approche de recherche qui étudierait la gestion des risques au sein du MDN/des FC de même que lorsqu'ils sont en relation avec d'autres organismes gouvernementaux susceptibles de prendre part à la réaction à des menaces terroristes. Finalement, ce rapport décrit l'élaboration de questionnaires de recherche qui pourraient être utilisés pour examiner plus en détail ces problèmes, et il présente les questions qui pourraient être utilisées au cours d'entrevues directes. D'autres approches de recherche possibles sont aussi examinées, notamment l'élaboration de scénarios de gestion des risques. Il y a lieu d'espérer que le travail entrepris dans le cadre de ce projet fournira un fondement solide pour les travaux de recherche futurs visant la compréhension et la promotion de niveaux d'interopérabilité plus élevés en ce qui a trait à la gestion des risques.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

(U) Risk, Risk management, Risk assessment, Interoperability, Terrorism prediction, Integrated risk management framework, CF doctrine; DND policy